UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM DESENVOLVIMENTO PARA DISPOSITIVOS MÓVEIS E INTERNET DAS COISAS

FELIPE RAFAEL MAIA RODRIGUES

SEGURANÇA E CONTROLE DO ARMAMENTO NAS CORPORAÇÕES MILITARES ATRAVÉS DA TECNOLOGIA MÓVEL E INTERNET DAS COISAS

Curitiba
2020

FELIPE RAFAEL MAIA RODRIGUES

SEGURANÇA E CONTROLE DO ARMAMENTO NAS CORPORAÇÕES MILITARES ATRAVÉS DA TECNOLOGIA MÓVEL E INTERNET DAS COISAS

Monografia de Especialização apresentada ao Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de “Especialista em Desenvolvimento para Dispositivos Móveis e Internet das Coisas”.

Orientador: Prof. João Alberto Fabro.

Curitiba

2020

Ministério da Educação
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Campus Curitiba
Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Informática
Coordenação do Curso de Especialização em Desenvolvimento para Dispositivos Móveis e Internet das Coisas

TERMO DE APROVAÇÃO

SEGURANÇA E CONTROLE DO ARMAMENTO NAS CORPORAÇÕES MILITARES ATRAVÉS DA TECNOLOGIA MÓVEL E INTERNET DAS COISAS

por

“Felipe Rafael Maia Rodrigues”

Este Trabalho de Conclusão de Curso foi apresentado as 10:00 do dia 17 de julho de 2020 por videoconferência como requisito parcial à obtenção do grau de Especialista em Desenvolvimento para Dispositivos Móveis e Internet das Coisas na Universidade Tecnológica Federal do Paraná - UTFPR - Campus Curitiba. O(a) aluno(a) foi arguido pela Banca de Avaliação abaixo assinados. Após deliberação, a Banca de Avaliação considerou o trabalho aprovado.

_____ Prof. João Alberto Fabro **(Presidente/Orientador – UTFPR/Curitiba)**	_____ Prof. Maria Claudia Figueiredo Pereira Emer **(Avaliador 1– UTFPR/Curitiba)**
_____ Prof. Leandro Batista de Almeida **(Avaliador 2 – UTFPR/Curitiba)**	

“A Ata de Aprovação assinada encontra-se na Coordenação do Curso.”

AGRADECIMENTOS

Agradeço ao Orientador, João Alberto Fabro, pelo auxílio e apoio técnico para o desenvolvimento deste trabalho.

DEDICATÓRIA

Dedico este trabalho de conclusão aos meus pais que nunca mediram esforços para prover e possibilitar o meu desenvolvimento constante, e à minha esposa que me incentivou e apoiou no alcance dos meus objetivos.

RESUMO

Com o objetivo de desenvolver um projeto que trouxesse benefício para as organizações policiais e militares, e consequentemente, para a sociedade, foi proposto uma solução que fornecesse uma melhoria na segurança nas áreas de reservas de material bélico, utilizando-se do desenvolvimento de um aplicativo para smartphones associado a um dispositivo de internet das coisas (IoT). Conforme pesquisas realizadas, nos últimos anos essas áreas têm sido alvo de diversos extravios, roubos e furtos, então viu-se a necessidade do aumento na segurança desses locais. Realizou-se uma entrevista com os responsáveis pelas reservas de material em 4 departamentos da Polícia Militar do Paraná, obtendo informações e definindo os requisitos, para assim, construir o trabalho. Visando a melhoria na segurança e controle, o projeto traz uma solução através de um dispositivo IoT que contém um sensor de presença, um leitor de cartão de acesso com identificação por rádio frequência (RFID) e um microcontrolador com acesso à internet sem fio. Essa tecnologia permite o monitoramento no interior das reservas de materiais bélicos, informando no aplicativo móvel instalado no smartphone do responsável, os acessos e invasões nas reservas, com isso, permitindo a fiscalização e gerenciamento desse ambiente, de forma instantânea. Foi então realizada uma avaliação da solução desenvolvida, através de questionários, que constataram a factibilidade da proposta em auxiliar no controle e na segurança das reservas. A pretensão com este projeto é ter aplicabilidade futura real com intuito de facilitar a atividade militar, gerar estatísticas a partir do banco de dados, diminuir os trabalhos manuais, auxiliar na segurança em tempo real e fornecer proteção no depósito, como também aos colaboradores envolvidos neste processo.

PALAVRAS – CHAVE: Internet das Coisas, Armamento, Aplicativo móvel, Segurança, Tecnologia.

ABSTRACT

In order to develop a project that would benefit the police and military organizations, and consequently, for society, a solution was proposed that would provide an improvement in security in the areas of war material reserves, using the development of an application for smartphones associated with an internet of things (IoT) device. According to research carried out, in recent years these areas have been the target of several losses, thefts and thefts, so there was a need to increase the security of these places. An interview was held with those responsible for material reserves in 4 departments of the Military Police of Paraná, obtaining information and defining the requirements, to build the work. Aiming at improving security and control, the project brings a solution through an IoT device that contains a presence sensor, an access card reader with radio frequency identification (RFID) and a microcontroller with wireless internet access. This technology allows the monitoring inside the war material reserves, informing in the mobile application installed on the responsible person's smartphone, the accesses and invasions in the reserves, thus allowing the inspection and management of this environment, instantly. An evaluation of the developed solution was then carried out, through questionnaires, which verified the feasibility of the proposal to assist in the control and security of reserves. The intention with this project is to have real future applicability in order to facilitate military activity, generate statistics from the database, decrease manual work, assist in real time security and provide protection in the warehouse, as well as the employees involved in this process.

KEYWORDS: Internet of things, armament, mobile application, security, technology.

LISTA DE FIGURAS

Figura 1. Metodologia.....22
Figura 2. ESP32 face 1.....25
Figura 3. ESP32 face 2.....25
Figura 4. Sensor PIR face 1.....26
Figura 5. Sensor PIR face 2.....27
Figura 6. Sensor PIR ESP32.....28
Figura 7. TAG e Sensor RFID.....29
Figura 8. Diagrama de conexão ESP32 e Sensor RFID.....30
Figura 9. Foto buzzer.....31
Figura 10. Diagrama ESP32 e buzzer.....31
Figura 11. Diagrama comunicação.....38
Figura 12. Diagrama de caso de uso “Detecta Movimento” 38
Figura 13. Notificação.....40
Figura 14. Diagrama de atividade do caso de uso “Detecta Movimento” 42
Figura 15. Diagrama de casos de uso do usuário com dispositivo IoT e com aplicativo móvel.....43
Figura 16. Diagrama de atividade do caso de uso “Aplicar TAG no leitor RFID” 45
Figura 17. Diagrama de estados do alarme.....46
Figura 18. Tela Inicial do aplicativo.....48
Figura 19. Tela de cadastro.....49
Figura 20. Diagrama de atividade do caso de uso “Cadastrar” 50
Figura 21. Tela do login.....52
Figura 22. Diagrama de atividade do caso de uso “Login” 53
Figura 23. Tela menu principal.....55
Figura 24. Tela de relatórios.....56
Figura 25. Tela escolha da data inicial.....57
Figura 26. Tela data final.....58
Figura 27. Tela relatório de acesso.....59
Figura 28. Tela relatório de disparos.....60
Figura 29. Objeto acessos.....61
Figura 30. Objeto disparo alarme.....62
Figura 31. Diagrama do banco de dados.....63
Figura 32. Diagrama de atividade do caso de uso “Gerar Relatório” 64
Figura 33. Tela lista de usuários.....66
Figura 34. Tela confirmação de exclusão.....67
Figura 35. Diagrama de atividade do caso de uso “Excluir Usuário” 68
Figura 36. Tela gerar token.....70
Figura 37. Tela mostra token.....71
Figura 38. Diagrama de classes.....72
Figura 39. Dispositivo IoT.....73

LISTA DE TABELAS

Tabela 1. Taxa de mortalidade por porte de arma de fogo - PAF no Brasil, segundo UF a ano, **1996-2006**.....17

Tabela 2. Entrevista Furriel.....32

Tabela 3. Entrevista Superior Direto.....33

Tabela 4. Teste e avaliação de usabilidade – Superiores.....74

Tabela 5. Teste e avaliação de usabilidade – Furriéis.....75

LISTA DE SIGLAS

IoT – *Internet of Things* (Internet das coisas)
PMPR - Polícia Militar do Paraná
PMSP - Polícia Militar de São Paulo
VAJME - Vara da Auditoria da Justiça Militar Estadual
COGER - Corregedoria Geral
RFID - *Radio-Frequency Identification* (Identificação por Rádio Frequência)
JSON - *JavaScript Object Notation* (Notação de Objetos do Javascript)
Sensor PIR – *Pyroelectric InfraRed sensor module* (Sensor infravermelho piroelétrico)
TAG – Sinônimo para cartão magnético
GPIO – *General Purpose Input/Output* (Pinos de comunicação de entrada e saída)
COE – Companhia de Comandos e Operações Especiais
1° CRPM – Primeiro Comando Regional de Polícia Militar
BOPE – Batalhão de Operações Especiais
CHOQUE – Companhia de Polícia de Choque
QCG – Quartel do Comando Geral

SUMÁRIO

1. INTRODUÇÃO 13
1.1 Justificativa 14
1.2 Objetivos 18
1.2.1 Objetivo Geral 18
1.2.2 Objetivos Específicos 18
1.2.3 Limitações 18
1.3 Organização do Documento 19
2. METODOLOGIA 20
3. FUNDAMENTAÇÃO TEÓRICA 23
3.1 Tecnologias 23
3.3.1 Firebase - Banco de dados 23
3.3.2 Android Studio - Ambiente de desenvolvimento mobile 23
3.3.3 Arduino IDE - Ambiente de desenvolvimento de microcontroladores 24
3.3.4 Dispositivo IoT 24
3.3.5 Microcontrolador - Esp32 24
3.3.6 Sensor de presença e movimento - Sensor PIR 26
3.3.7 Leitor da TAG - sensor RFID 28
3.3.8 Buzzer 30
4. DESENVOLVIMENTO 32
4.1 Entrevista - Coleta de requisitos 32
4.2 Descrição do Projeto 34
4.3 Levantamento de requisitos 34
4.3.1 Requisitos funcionais 35
4.3.2 Requisitos não-funcionais 36
4.4 Implementação 37

4.5 Validação do Projeto 73
5. CONCLUSÃO E TRABALHOS FUTUROS 76
5.1 TRABALHOS FUTUROS 77
6. REFERÊNCIAS 78
7. APÊNDICES 81
7.1 APÊNDICE A – Gráfico de Gantt Parte 1 81
7.2 APÊNDICE B – Gráfico de Gantt Parte 2 82

1. INTRODUÇÃO

Atualmente os depósitos de materiais bélicos são supervisionados por um ou mais militares, sempre gerenciados por um superior hierárquico direto. Todo o controle de acesso, além da entrega e recebimento de armamentos e munições, é realizado manualmente, através de documentos físicos e planilhas. A segurança é mantida por meios mecânicos e dependentes de cautela humana. É preciso, segundo o RISG PMPR - (Regulamento Interno e dos Serviços Gerais da PMPR, decreto 7339, Art. 220).

> Ao P/4 incumbe I - desenvolver as atividades de administração de materiais, de semoventes, munições, explosivos e armamentos, primando pela eficiência e continuidade de funcionamento do sistema de comunicações da unidade.

Analisando os procedimentos realizados neste momento, foi identificado que a tecnologia da informação pode auxiliar no melhor controle, apoiar a segurança tanto departamental quanto às pessoas envolvidas, agilizar as atividades e a troca de informações e atender na efetividade do gerenciamento destes processos. Segundo o RISG PMPR - (Regulamento Interno e dos Serviços Gerais da PMPR), decreto 7339, Art. 214): “Ao Comandante de Unidade incumbe XXXI - Participar, de imediato, ao escalão superior qualquer extravio, furto ou roubo de armamento, munição ou explosivo da unidade”.

Os benefícios de associar novas tecnologias com qualquer instituição, são vistos há tempos por todas as partes interessadas. Segundo (SANTOS, 2019) o surgimento da computação em nuvem faz com que empresas possam solucionar problemas antes insolúveis, com uma velocidade e agilidade muito maior.

Desta forma o estudo e desenvolvimento deste trabalho, pretende criar uma solução para o controle do armazenamento seguro de materiais bélicos em quartéis, por meio da elaboração de um aplicativo móvel para smartphones Android, integrado a um dispositivo IoT (*Internet of Things*-Internet das Coisas) desenvolvido especificamente para este fim, e através do banco de dados em nuvem. Futuramente planeja-se a apresentação e implementação desse projeto, nas organizações militares interessadas; atualmente não existem projeções de

utilização dele. Através de entrevistas, serão definidos os requisitos e benefícios do sistema, com o objetivo de levar a real eficiência na segurança, tanto dos materiais quanto das pessoas. Segundo o decreto RISG PMPR - (Regulamento Interno e dos Serviços Gerais da PMPR, decreto 7339, Art. 220).

> Ao P/4 incumbe XII - propor as medidas de segurança que se fizerem necessárias para reservas ou depósitos de armamentos e combustíveis no que tange às condições de segurança do material e do pessoal que deve manuseá-los.

1.1 Justificativa

Segundo a mídia independente Ponte, focada em segurança pública, dados coletados diretamente via LAI - Lei de Acesso sobre a Informação, escrito por (MOREIRA, 2019) “revelam que entre 2010 e agosto de 2018, 600 armas da marca Taurus foram roubadas, extraviadas ou furtadas da Polícia Militar de São Paulo”. Conforme o mesmo órgão, a média de prejuízo aos cofres públicos em 8 anos de desvio foi de R$ 1,4 milhão. Esses números apontam a importância de um sistema para auxiliar na fiscalização de tais bens. As referências citadas são apenas da Polícia Militar de São Paulo, assim ao expandir esta estimativa para o âmbito nacional, e para as demais forças de segurança, tais registros podem ser muito maiores, o que os torna alarmantes.

Conforme Samira Bueno, diretora executiva do FBSP (Fórum Brasileiro de Segurança Pública), em entrevista para a mídia Ponte, enfatiza que o desaparecimento é reflexo de um controle pouco eficiente dos estoques de armas da corporação. Sendo assim, o objetivo deste trabalho visa a instalação de um dispositivo IoT contendo um sensor de movimento silencioso no interior da reserva, informando a invasão através de comunicação sem fio, para o superior direto e/ou uma equipe de segurança do local, contribuindo em tempo real, por meio de um aplicativo mobile, o fluxo de informações dentro de tais dependências.

Através de pesquisa também exploratória foram encontradas diversas notícias a respeito do assunto tratado. Um dos eventos encontrados, ocorrido entre os anos de 2012 a 2014 no estado do Paraná, com o ex - furriel do almoxarifado do 1°CRPM, acusado de realizar peculato por 10 vezes, resultando

no desvio de mais de 70 armas de fogo, conforme Tribunal de Justiça do Paraná TJ-PR.

Este problema gera impactos negativos a toda a sociedade, pois essas armas se transformam em instrumentos criminais, provendo o aumento de morte por arma de fogo, conforme apresenta a Tabela 1 – página 17 – percebe-se que nos anos de 1996, 1997, 2000, 2002 até 2005 o estado do Rio de Janeiro manteve a maior taxa comparado aos demais estados. Pernambuco nos anos de 1998, 1999, 2001 e 2006 obteve maior índice. O projeto visa apoiar a segurança tanto na prevenção de obtenção de materiais bélicos por criminosos, quanto para os militares que trabalham na supervisão destes. Existem dois fatores a serem tratados para proteção dos envolvidos:

- **Proteção jurídica:** no caso de investigação por parte de extravio ou peculato, é realizada uma investigação, por ser um processo manual atualmente isto se torna moroso por falta de apoio eletrônico, assim pode haver acusações sem fundamentos. Um exemplo é o caso ocorrido em 2012 a 2014, julgado no Tribunal de Justiça do Paraná TJ-PR. O réu relata que “desconhece quem tenha sido o responsável pelo sumiço das armas mencionadas na denúncia; (...) que muitas pessoas tinham acesso àquela seção, ao almoxarifado do 1°CRPM, bem como chaves do cofre e do armário”.

  Subentende-se que mais de uma pessoa pode ter realizado o crime, dificultando a investigação.

- **Proteção à vida:** No caso do militar ser rendido por criminosos durante a guarda e ser obrigado a abrir a reserva, pelo processo atual não existe nenhum sistema de alarme para auxiliar as análises, por parte do superior, sobre avisos de entradas não autorizadas no local da reserva.

Além disso, pesquisas foram realizadas a respeito de soluções semelhantes, dentro de organizações policiais e militares, sobre um sistema de segurança nos depósitos de material bélico, porém nada foi encontrado nesse sentido.

O propósito das corporações de segurança pública é de fornecer proteção a sociedade, este projeto juntamente com essa missão tão importante, poderá elevar o nível de força no combate contra o crime e a favor a vida.

Tabela 1. Taxa de mortalidade por porte de arma de fogo - PAF no Brasil, segundo UF a ano, 1996-2006.

UF de Ocorrência	Taxas por 100.000 habitantes											Percentuais				
	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	Nível médio	Nível médio padronizado	Tendência 1996-2001 / 2002-2006	Tendência 1996 / 2006	Tendência 2003 / 2006
Rondônia	22,4	21,1	25,9	25,4	21,9	29,5	28,5	27,9	24,8	26,9	26,5	25,5	55,5%	10,4%	18,6%	-5,1%
Acre	14,9	15,1	15,0	9,6	8,8	11,7	13,1	9,4	9,7	6,9	8,3	11,1	24,2%	-24,2%	-44,5%	-12,1%
Amazonas	10,3	9,0	9,5	8,9	9,3	7,7	7,3	6,5	8,1	8,9	11,8	8,9	19,2%	-6,3%	15,2%	80,9%
Roraima	19,1	14,9	21,0	21,4	16,0	14,0	16,4	12,5	12,4	9,9	10,4	15,3	33,2%	-30,6%	-45,8%	-17,1%
Pará	6,7	8,1	8,9	7,9	8,5	9,9	11,4	13,8	15,2	18,2	19,9	11,7	25,4%	88,5%	197,6%	44,4%
Amapá	23,6	14,7	17,5	13,4	8,6	10,0	10,2	14,6	13,7	9,6	12,6	13,5	29,3%	-16,8%	-46,6%	-13,8%
Tocantins	7,9	7,0	9,6	9,6	10,7	14,2	8,7	11,7	9,5	7,8	8,8	9,6	20,8%	-5,6%	11,7%	-24,8%
Maranhão	4,3	3,7	4,4	3,1	3,6	4,5	4,9	6,3	6,1	8,6	8,6	5,3	11,5%	75,6%	101,1%	36,0%
Piauí	2,5	2,5	2,5	2,8	4,7	5,1	5,4	6,8	6,1	6,2	8,1	4,8	10,4%	94,3%	229,1%	19,1%
Ceará	6,4	7,4	7,6	8,0	9,4	9,4	10,6	11,7	12,1	13,3	13,9	10,0	21,7%	54,0%	118,5%	19,5%
Rio Grande do Norte	9,8	10,8	7,9	8,7	9,8	11,1	10,6	11,8	12,7	13,9	15,4	11,1	24,2%	33,1%	57,4%	30,5%
Paraíba	8,1	10,2	9,5	8,2	11,5	10,6	12,9	13,7	13,7	15,9	18,2	12,0	26,1%	53,8%	125,1%	33,0%
Pernambuco	32,4	40,9	48,6	47,3	46,6	50,2	46,4	46,6	41,1	42,5	43,4	44,2	96,0%	-0,7%	34,0%	-6,9%
Alagoas	20,0	18,0	15,6	14,2	17,5	21,8	25,0	26,7	25,7	30,8	43,3	23,5	51,0%	70,0%	116,6%	62,0%
Sergipe	13,5	10,1	11,2	15,8	17,2	22,2	22,4	19,3	16,6	17,1	21,4	17,0	36,9%	28,9%	58,2%	11,0%
Bahia	12,2	11,9	13,1	11,5	11,6	13,2	15,5	17,1	16,6	17,3	19,1	14,5	31,4%	39,7%	56,6%	11,1%
Minas Gerais	6,3	6,7	7,5	5,7	8,9	9,6	12,0	15,9	18,0	17,0	16,7	11,3	24,6%	113,6%	165,5%	4,9%
Espírito Santo	25,7	34,5	40,7	38,5	33,3	33,6	38,7	37,2	36,6	36,1	38,6	35,8	77,7%	8,9%	50,4%	4,0%
Rio de Janeiro	46,4	46,8	47,1	46,5	47,1	46,1	49,3	47,6	45,5	43,4	40,9	46,0	100,0%	-2,8%	-11,8%	-14,2%
São Paulo	17,4	16,9	19,3	23,6	28,7	30,4	26,8	26,3	20,9	16,2	15,7	22,0	47,8%	-6,6%	-9,9%	-40,5%
Paraná	12,0	12,2	13,0	13,0	13,6	15,8	17,1	19,5	20,9	21,5	22,9	16,5	35,8%	53,3%	91,2%	17,4%
Santa Catarina	6,0	6,9	6,2	5,7	6,1	6,8	7,6	8,9	8,0	8,0	7,6	7,1	15,4%	27,3%	26,7%	-14,7%
Rio Grande do Sul	15,4	15,9	14,9	15,1	16,3	16,2	16,6	16,4	16,3	16,3	16,3	16,0	34,7%	4,8%	5,8%	-0,9%
Mato Grosso do Sul	28,8	28,8	22,9	19,6	23,9	20,9	22,1	22,2	19,1	17,6	18,6	22,2	48,3%	-17,4%	-35,3%	-16,2%
Mato Grosso	21,9	20,4	25,2	21,2	29,8	24,8	25,0	24,5	19,2	19,7	19,7	22,9	49,6%	-9,4%	-10,1%	-19,8%
Goiás	13,4	13,1	13,1	15,9	15,6	15,9	18,0	16,6	18,0	17,3	17,3	15,8	34,4%	20,4%	28,7%	4,0%
Distrito Federal	30,1	27,1	29,2	26,4	28,8	27,9	26,5	29,8	26,6	23,3	22,0	27,1	58,8%	-9,3%	-26,9%	-26,0%
Brasil	**16,6**	**17,1**	**18,3**	**18,7**	**20,6**	**21,6**	**21,8**	**22,4**	**20,9**	**20,0**	**20,4**	**19,9**	**43,1%**	**12,1%**	**23,1%**	**-8,8%**

Fonte: Sistema de Informação sobre Mortalidade (SIM) – DATASUS/MS Análise: Pesquisa, Viva Comunidade e Congresso em foco, pág. 9.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo deste trabalho é desenvolver uma solução, baseada em dispositivos de IoT e aplicativo móvel, que possa prover maior segurança e controle de acesso aos depósitos de armamentos de instituições policiais e das forças armadas.

1.2.2 Objetivos Específicos

Para que o Objetivo Geral seja alcançado, é preciso atingir os seguintes objetivos específicos:

a) Realizar um levantamento de casos de extravio, furto e roubo de depósitos de armamentos;
b) Estudar a metodologia de segurança, processo atual;
c) Aplicação de entrevista com os responsáveis e colaboradores da área – coleta de requisitos;
d) Estabelecer quais requisitos serão atendidos;
e) Definir aplicativo móvel e recursos a serem utilizados;
f) Desenvolver projeto incluindo: dispositivo de IoT, aplicativo móvel e a interconexão entre ambos, relatórios de acessos e disparos do alarme.
g) Testar a funcionalidade com possíveis usuários;

1.2.3 Limitações

Este estudo e desenvolvimento limita-se aos materiais bélicos sob cautela das reservas militares, que representa de maneira geral o sistema de segurança, sem personalizar neste momento, qualquer tipo de instituição ou região específica. Este projeto não viabiliza relatórios individuais a respeito de cada armamento, no seu fluxo de entrada e/ou saída dos locais de armazenamento. Este projeto também limita-se ao desenvolvimento do aplicativo móvel apenas para a plataforma Android.

1.3 Organização do Documento

O restante deste documento está organizado da seguinte forma:

- Seção 2 Metodologia, é apresentada a estrutura de execução do projeto;
- Seção 3 Fundamentação teórica, são apresentadas as tecnologias empregadas;
- Seção 4 Desenvolvimento, são apresentadas as entrevistas, a descrição do projeto, os requisitos funcionais e não funcionais e a implementação com: diagramas, casos de uso, e testes e validações.
- Seção 5 - Conclusões e trabalhos futuros, são apresentadas as conclusões obtidas a partir do desenvolvimento do projeto, e possíveis melhorias e avanços que podem ser feitos em futuras versões.

2. METODOLOGIA

O fluxograma apresentado na Figura 1 – página 22 – foi desenvolvido para tornar visível a sequência geral do projeto. Cada etapa do desenvolvimento do trabalho é detalhada nesta seção.

A **pesquisa inicial** sobre o tema foi realizada no ambiente militar da PMPR, sobre o alinhamento das informações sigilosas e limites a serem demonstrados durante o projeto. Foi feito então o levantamento de possíveis problemas a serem tratados, com o propósito de entregar real valor aos órgãos públicos, prezando sempre o bem da sociedade e respeitando o sistema atual.

Foi identificada a possibilidade de melhoria na segurança e controle dos depósitos de material bélico, pois na maioria dos casos o método realizado atualmente não possui tecnologia eletrônica no apoio aos envolvidos. A falta desse sistema pode acarretar a facilidade de peculato, furtos, roubos com a rendição da equipe de serviço, morosidade no controle dos insumos e demora na geração de relatórios.

Na etapa de **coleta de dados sobre o projeto**, foi avaliada a real importância desta construção. Somente a VAJME (Vara da Auditoria da Justiça Militar Estadual) e a COGER (Corregedoria Geral), possuem informações oficiais a respeito de quantidade e casos de armamento extraviados. No geral existem relatos que existem aproximadamente 516 desvios nos últimos anos, porém a criação desses relatórios é feita manualmente e não possui detalhamento com especificações de cada situação.

Na fase de **coleta de requisitos**, focou-se em apenas uma organização. Cada instituição pública de segurança tem sua reserva de material bélico. Essas organizações podem ser Polícia Militar, Exército Brasileiro, Polícia Civil, Guarda Municipal, entre outros. Este trabalho foi baseado principalmente na PMPR pois havia maior acesso às informações sigilosas e públicas, uma vez que o autor desse projeto faz parte a corporação desde 2013.

Visando a compreensão do modo como é realizado o trabalho nos depósitos, foi desenvolvido um questionário com o objetivo de coletar informações diretamente dos militares que trabalham nessas áreas, através da aplicação de uma entrevista que obteve dados qualitativos e quantitativos. O objetivo geral dessa é etapa é entender as necessidades reais desta função,

para que o desenvolvimento da solução seja efetivo. Os resultados serão apresentados na seção 4.1.

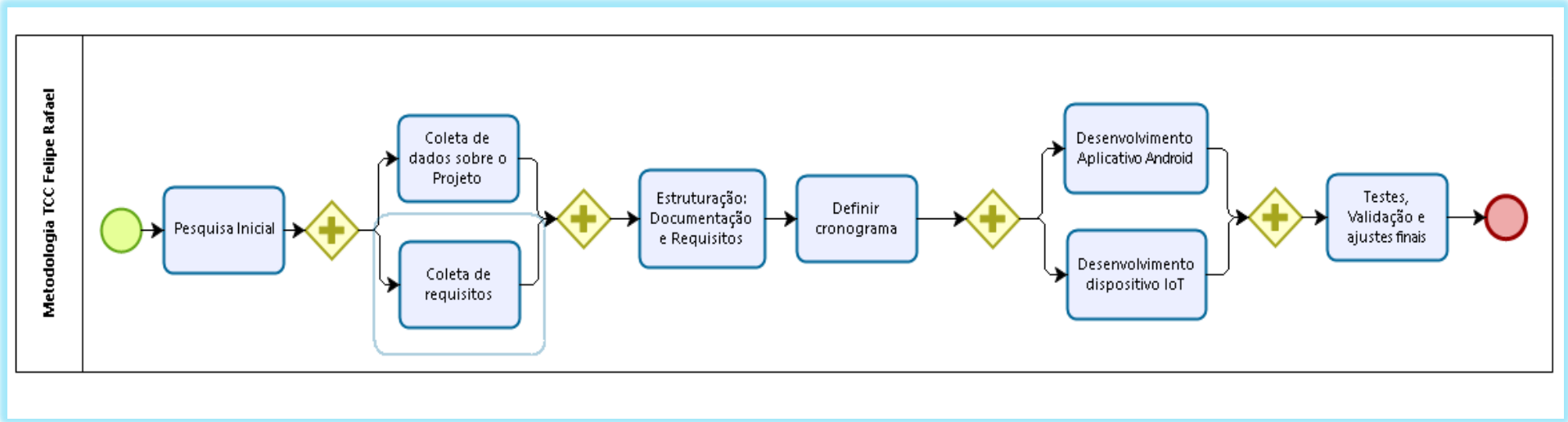
Na fase de **estruturação**, foi realizada a busca de embasamento teórico para o desenvolvimento do trabalho, de acordo com os requisitos da solução levantados. Nos Apêndices A e B do trabalho, é apresentado o **cronograma** através do gráfico de Gantt com os marcos de entrega.

As etapas de **desenvolvimento do App Android** e **dispositivos IoT**, foram subdivididas em diversas atividades, para atender a todos os objetivos desse projeto. Algumas foram feitas em paralelo, para que houvesse integração. Especificamente seguem os marcos das entregas:

1. 1° Entrega documentação;
2. 1º Fase Desenvolvimento Android;
3. Desenvolvimento do dispositivo IoT;
4. 2º Fase Desenvolvimento Android.

Na fase de **testes, validação e ajustes finais**, foi feito primeiramente um teste de funcionalidade com os entrevistados, para colher sugestões e avaliação de 0 a 5 por sua usabilidade. Por fim, foi feita a validação e ajustes finais de todo o trabalho, buscando falhas ou lacunas não implementadas, para entregar um projeto de segurança e controle de acessos a depósitos de armamentos o mais funcional possível.

Figura 1. Metodologia.



Fonte: Desenvolvido pelo Autor.

3. FUNDAMENTAÇÃO TEÓRICA

3.1 TECNOLOGIAS

O projeto conterá sensor de movimento aliado ao leitor de RFID que irá ativar e desativar a detecção de movimento silenciosa. O aplicativo mobile será produzido para o sistema operacional Android na linguagem de programação Java e utilizando o ambiente de desenvolvimento integrado Android Studio.

No estudo das necessidades do projeto, visando cumprir todos os objetivos propostos com máxima qualidade e confiabilidade, foi imprescindível o uso das seguintes tecnologias:

3.3.1 Firebase - Banco de dados

Segundo (VIANA; Daniel, 2017)

> Firebase é uma plataforma do Google que contém várias ferramentas e uma excelente infraestrutura para ajudar desenvolvedores web e mobile a criar aplicações de alta qualidade e performance.

Firebase é um banco de dados em tempo real, ou seja, cada alteração feita nos dados é visualizável imediatamente por todos os dispositivos conectados ao banco; também é capaz de armazenar arquivos como: fotos e documentos. Possui fácil configuração e entre suas ferramentas contém a geração de notificações, que será muito utilizada nesse projeto.

3.3.2 Android Studio - Ambiente de desenvolvimento mobile

Com base em (HARADA; 2019), o Android Studio é chamado de Ambiente de Desenvolvimento Integrado, um programa de computador que reúne as características e ferramentas de apoio para a criação de aplicativos para dispositivos móveis que são executados no sistema operacional Android.

3.3.3 Arduino IDE - Ambiente de desenvolvimento de microcontroladores

Conforme (MOTA, 2017), o Arduino IDE “[...] é um software onde podemos escrever um código em linguagem semelhante a C/C++, o qual, será traduzido, após a compilação, em um código compreensível[...]” pelo microcontrolador, em que esse fará a leitura e execução desses comandos.

Arduino IDE é gratuito e compatível com sistemas operacionais Windows e Linux, também notifica o desenvolvedor a respeito do projeto apresentar algum problema em sua configuração ou até mesmo em seu código, (STRAUB, 2019).

3.3.4 Dispositivo IoT

O dispositivo IoT é a junção de vários componentes de IoT com o intuito de fornecer uma solução específica, no caso desse projeto ele é composto por microcontrolador, sensor de movimento e leitor da TAG (cartão magnético).

3.3.5 Microcontrolador - Esp32

Segundo (LOCATELLI, 2020) no Blog da Curto, o ESP32 apresenta-se como um meio inovador no desenvolvimento de projetos automatizados. Esse pequeno componente apresenta módulo de comunicação Wi-Fi, um sistema com processador Dual Core, Bluetooth híbrido e múltiplos sensores embutidos, tornando a construção de sistema como internet das coisas (IoT) muito mais simples e compacto, além de ter baixo custo e alto desempenho.

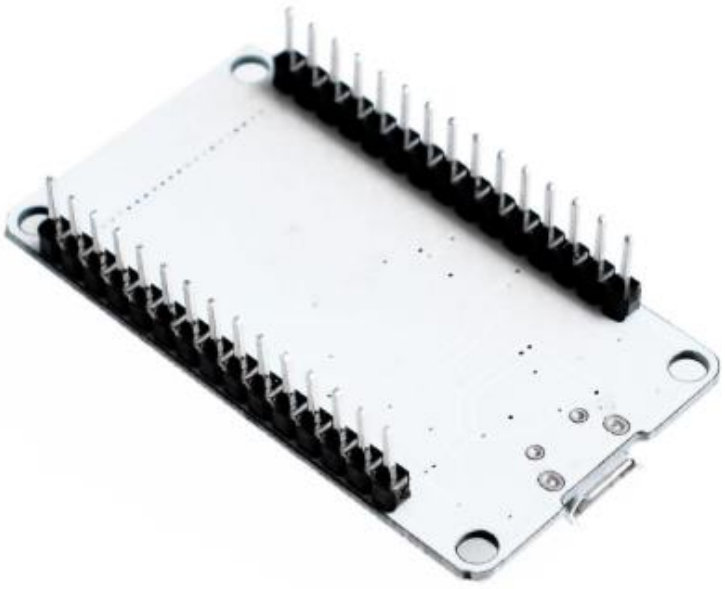
O microcontrolador funciona de modo semelhante a um computador, ele executará os comandos enviados de um aplicativo previamente instalado.

Nas Figuras 2 e 3 são apresentadas duas visões da placa ESP32 utilizada neste projeto. Esta placa possui as dimensões de 55 x 27 mm.

Figura 2. ESP32 face 1.

Fonte: Página Usinainfo. Disponível em: < https://www.usinainfo.com.br/nodemcu/esp32-nodemcu-iot-com-wifi-e-bluetooth-30-pinos-5147.html>. Acesso em: 22 jul. 2020.

Figura 3. ESP32 face 2.



Fonte: Página Usinainfo. Disponível em: < https://www.usinainfo.com.br/nodemcu/esp32-nodemcu-iot-com-wifi-e-bluetooth-30-pinos-5147.html>. Acesso em: 22 jul. 2020.

3.3.6 Sensor de presença e movimento - Sensor PIR

Conforme (REIS, 2018):

> Um sensor de movimento PIR é, basicamente, uma câmera infravermelha que detecta a radiação IR (“radiação de corpo negro”) que é irradiada por objetos que penetram em seu campo de visão. No geral, esse tipo de sensor capta radiação infravermelha com comprimento de onda em torno de 10μm (10 micrômetros, equivalente a 10.000nm), que equivale aproximadamente à temperatura corporal de animais de sangue quente em geral, como os seres humanos.

Pode captar qualquer corpo com temperatura entre -20°C e 80°C que esteja em uma área de até 7m².

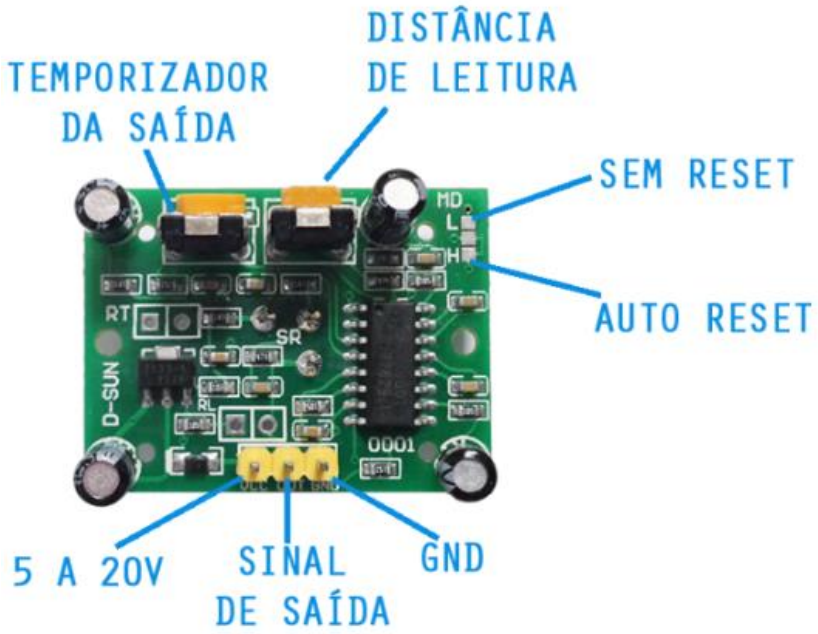
Os sensores são utilizados na maioria dos casos em ambientes empresariais e domésticos, onde contemplam, no geral, as finalidades: acender luzes automaticamente, disparo de alarmes, abrir portas e acionar dispositivo de captura de imagem. O seu consumo é amplo, pois sua dimensão é pequena, é barato, a conectividade é fácil, apresenta alta durabilidade, utiliza pouca energia e sua implementação é descomplicada. O sensor utilizado neste projeto é apresentado na Figura 4, e possui dimensões de 32 x 24 mm.

Quando o sensor identifica a radiação infravermelha, ele emite um sinal elétrico por uma de suas portas de comunicação; conforme apresentado na Figura 5 no local “sinal de saída”. Esta porta é conectada ao microcontrolador para que receba a informação, vinda através do sinal do sensor, de que houve uma movimentação no local.

Figura 4. Sensor PIR face 1.

Fonte: Página Usinainfo. Disponível em: < https://www.usinainfo.com.br/sensor-de-movimento/sensor-pir-sensor-de-movimento-para-arduino-hc-sr501-2634.html>. Acesso em: 22 jul. 2020.

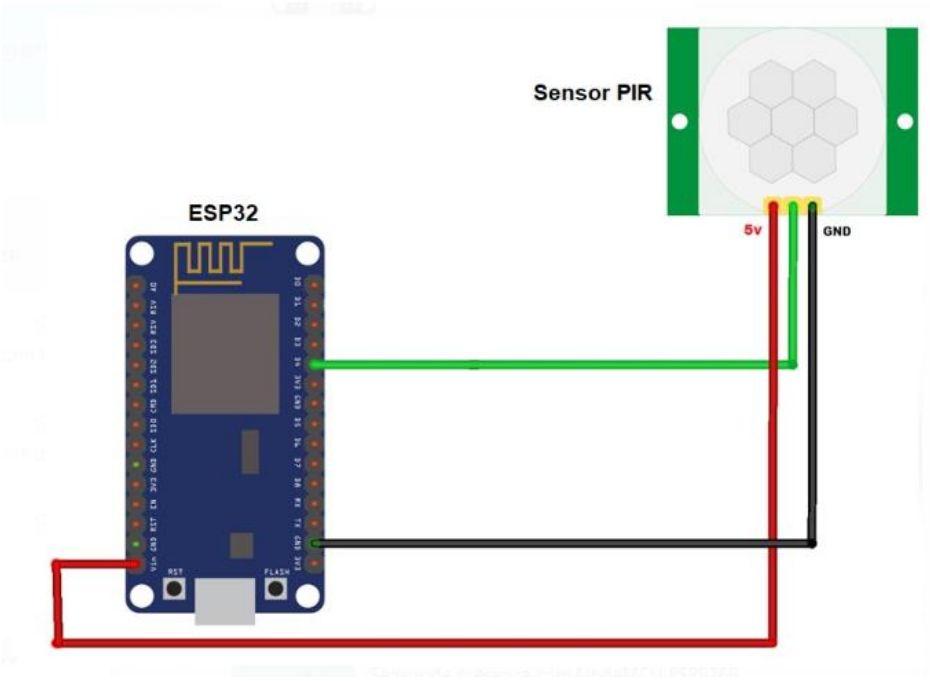
Figura 5. Sensor PIR face 2.



Fonte: Robocore. Disponível em: <https://www.robocore.net/loja/sensores/sensor-de-presenca-pir-hc-sr501?gclid=EAIaIQobChMIvC_ouaW6gIVlYWRCh38PwBNEAQYASABEgLUXfD_BwE>. Acesso em: 22 jul. 2020.

A Figura 6, representa a conexão entre o sensor PIR e o microcontrolador. A linha preta e a vermelha representam, respectivamente, o polo negativo e o positivo, que fornecem energia para o funcionamento do sensor. A linha verde representa a conexão da porta sinalizadora do sensor PIR com uma porta "GPIO" do microcontrolador, ou seja, a partir dela que o ESP32 recebe o sinal da identificação de movimento.

Figura 6. Sensor PIR ESP32.



Fonte: Imagem modificada, baseada no site Fernando K. Tutoriais, Tecnologia e Tendências. Disponível em: <https://www.fernandok.com/2017/11/sensor-de-presenca-com-nodemcu-esp8266.html>. Acesso em: jun. de 2020.

3.3.7 Leitor da TAG - sensor RFID

Com base em (CIRIACO, 2009), a Radio Frequency IDentification, em português, Identificação por rádio frequência, é:

> [...] composto, basicamente, de uma antena, um transceptor, que faz a leitura do sinal e transfere a informação para um dispositivo leitor e um transponder ou etiqueta de RF (rádio frequência), que deverá conter o circuito e a informação a ser transmitida.

O cartão magnético – TAG, possui as informações que serão transmitidas para o leitor, podem ser encontradas no geral em dispositivos para abertura de portões, coleira de animais domésticos, nas embalagens, em produtos e dispositivos para ativação de diversos tipos de sistemas.

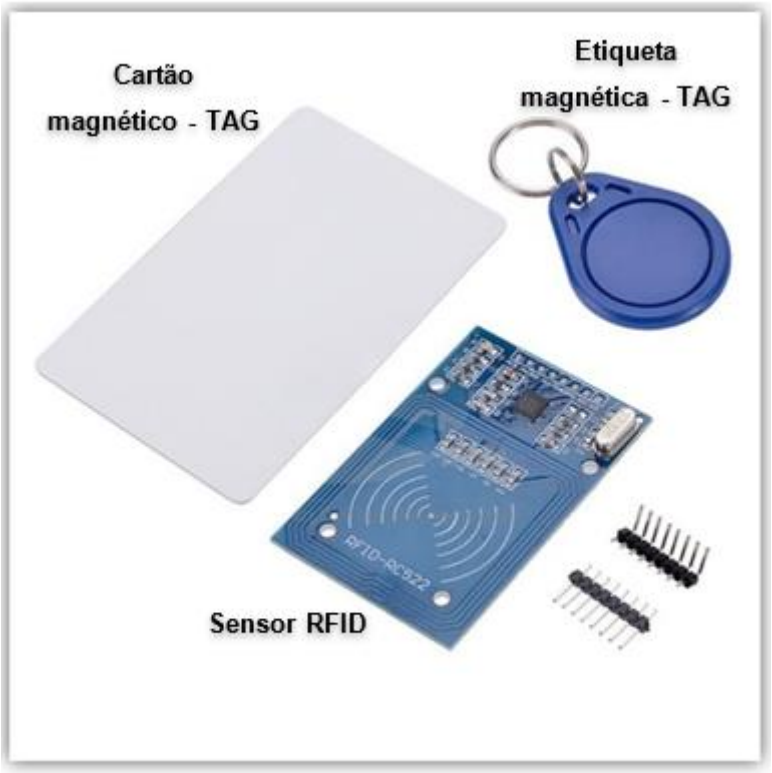
A TAG e o sensor são explicados tecnicamente por (CIRIACO, 2009):

> [...] a antena transmite a informação, emitindo o sinal do circuito integrado para transmitir suas informações para o leitor, que por sua vez converte as ondas de rádio do RFID para informações digitais. Agora,

depois de convertidas, elas poderão ser lidas e compreendidas por um computador para então ter seus dados analisados.

A seguir, a Figura 7 mostra os componentes desta tecnologia.

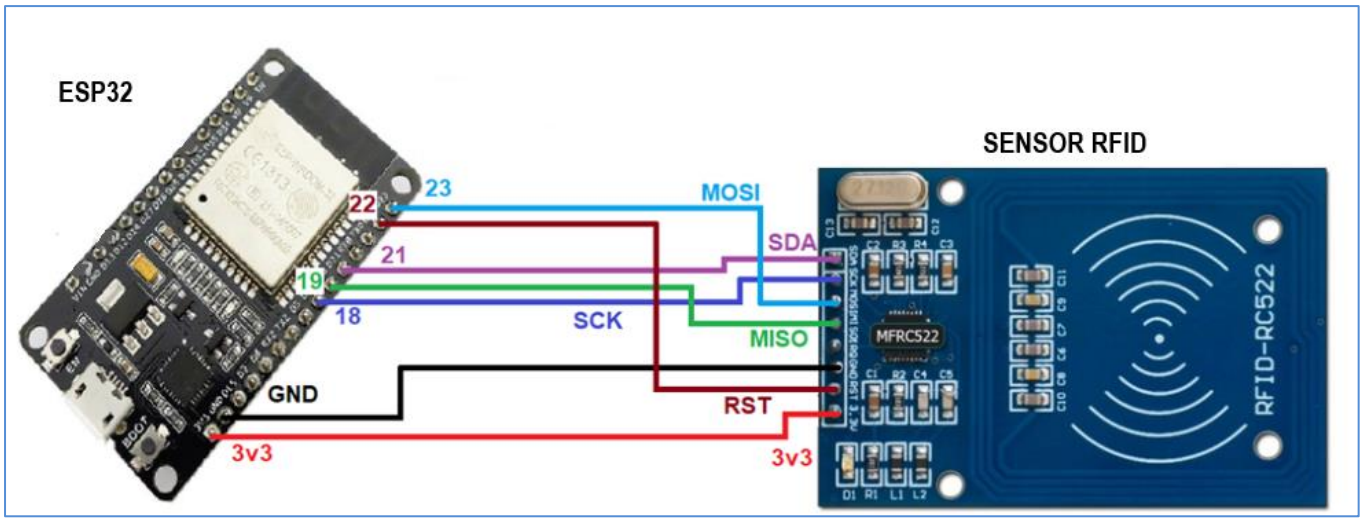
Figura 7. TAG e Sensor RFID.



Fonte: Imagem modificada pelo autor, com base na página Fernando K. Disponível em: < https://www.fernandok.com/2018/02/esp32-com-rfid-controle-de-acesso.html>. Acesso em: 22 jul. 2020.

O diagrama de conexão apresentado na Figura 8, mostra a linha vermelha e a preta representando, respectivamente, a ligação dos polos positivo e o negativo que fornecem energia para o funcionamento do sensor RFID. As demais conexões representam fluxo de dados, quando há a leitura da TAG.

Figura 8. Diagrama de conexão ESP32 e Sensor RFID.



Fonte: Imagem modificada pelo autor, com base na página Fernando K. Disponível em: < https://www.fernandok.com/2018/02/esp32-com-rfid-controle-de-acesso.html>. Acesso em: 22 jul. 2020.

3.3.8 Buzzer

O buzzer é um componente amplamente utilizado na robótica para alertar sonoramente a respeito de alguma informação ou acontecimento em um sistema. Entre suas utilizações estão: despertadores, alarmes e avisos de sistemas automotivos. Possui em seu interior um cristal Piezoeléctrico, que é o componente responsável por produzir o som.

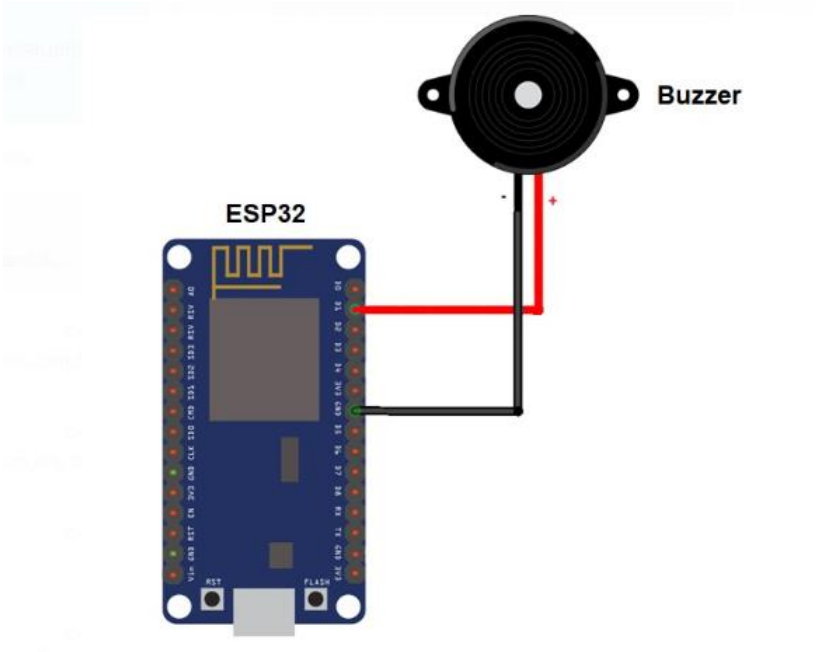
Conforme (CORREA, 2015) “Buzzer é um componente eletrônico que é composto por 2 camadas de Metal e uma terceira camada interna de cristal Piezoelétrico, este componente recebe uma fonte de energia e através dela emite uma frequência sonora”. A Figura 9 apresenta o componente utilizado neste projeto, que possui um diâmetro de 12 mm.

Figura 9. Foto buzzer.

Fonte: Página StellaSoft Tecnologia em Dados da Informação. Disponível em: <https://www.satellasoft.com/?materia=beep-usando-buzzer-com-arduino>. Acesso em: jun. de 2020.

A Figura 10 exemplifica uma conexão, onde a linha preta representa a ligação do polo negativo do buzzer com a porta "GND" do microcontrolador e a linha vermelha representa a conexão do polo positivo com uma porta "GPIO" do microcontrolador. Portanto, quando o microcontrolador envia um sinal elétrico pela porta "GPIO", o buzzer emite o som.

Figura 10. Diagrama ESP32 e buzzer.



Fonte: Imagem modificada, baseada no site Fernando K. Tutoriais, Tecnologia e Tendências. Disponível em: <https://www.fernandok.com/2017/11/sensor-de-presenca-com-nodemcu-esp8266.html>. Acesso em: jun. de 2020.

4. DESENVOLVIMENTO

4.1 ENTREVISTA - COLETA DE REQUISITOS

Através das entrevistas foram definidos quais métodos e recursos seriam desenvolvidos no projeto, para entregar real valor às corporações. A entrevista foi aplicada aos soldados e superiores dos locais com armamento do Quartel do Comando Geral da Polícia Militar do Paraná. As perguntas foram divididas em duas partes.

A primeira é a entrevista com o furriel, geralmente é um soldado responsável por realizar todos os trâmites de controle, documentação e fluxos de entrada e saída. É quem realiza de fato o monitoramento da segurança dessas áreas, todas as alterações que dizem respeito a reserva são repassadas ao seu superior direto. A seguir a tabela 2 mostra as perguntas e as respostas dos soldados:

Tabela 2. Entrevista Furriel.

Perguntas Furriel	**1º CRPM**	**COE**	**CHOQUE**	**BOPE**
	Respostas			
É interessante possuir um sistema eletrônico para auxiliar na segurança da reserva de materiais?	sim	sim	sim	Sim
O que esse sistema poderia fornecer? Exemplo: biometria, cartão magnético, sirene, sensor movimento, controle por celular etc.	sensor de movimento	biometria e sensor de movimento	biometria e sensor de movimento	sensor de movimento e controle pelo celular
Pontue a importância de um controle melhor na segurança das reservas de materiais, de 0 a 10. (Sendo 0 menor importância e 10 maior).	10	10	10	10

Fonte: Desenvolvido pelo Autor.

Foram entrevistados os furriéis dos seguintes departamentos: 1°CRPM – Primeiro Comando Regional da Polícia Militar, COE – Companhia de Comandos e Operações especiais, CHOQUE – Companhia de Polícia de Choque e o BOPE – Batalhão de Operações Especiais.

As respostas foram similares, quanto a importância deste projeto, no geral foi ressaltada a necessidade de um sistema eletrônico, para o auxílio da função, pois necessitam exercer grande atenção no fluxo do armamento e monitoramento dos locais, com a automação do monitoramento além da obtenção de maior segurança, é possível equilibrar melhor o esforço do trabalho.

A segunda é a entrevista com o superior direto, na maioria dos casos são militares com os cargos de Sargento, Tenente e Capitão. São responsáveis por prover recursos, viabilizando esse trabalho, como também garantir que a fiscalização desses materiais é eficaz e verdadeira. A seguir a tabela 3 mostra as perguntas e respostas dos superiores:

Tabela 3. Entrevista Superior Direto.

Perguntas Superior	**1° CRPM**	**COE**	**CHOQUE**	**BOPE**
	Respostas			
É interessante possuir um sistema eletrônico para auxiliar na segurança da reserva de materiais?	sim	sim	sim	sim, principalmente para os responsáveis que trabalham 24h nesta atividade
Gostaria de ter informações rápidas/relatórios, a distância e em tempo real sobre os acessos à reserva?	sim	sim	sim	Atualmente não enxerga necessidade
Pontue a importância de um controle melhor na segurança das reservas de materiais, de 0 a 10. (Sendo 0 menor importância e 10 maior).	10	10	10	10

Fonte: Desenvolvido pelo Autor.

A segunda entrevista foi aplicada com os superiores dos furriéis que participaram da primeira, assim foram mantidos os departamentos. Houve alteração na segunda questão da pesquisa, a fim de coletar a visão específica desta função, principalmente no quesito de coleta de informações ou relatórios de acesso.

As respostas foram a favor da implementação do projeto, dentre as considerações dos superiores, foi citado o grande passo que geraria na gestão das informações sobre o acesso aos locais, através da possibilidade de visualização de relatórios pelo aplicativo. O superior responsável pelo BOPE, relatou que neste departamento não havia fluxo significativo para a implementação deste sistema, mas afirmou que nos locais com funcionamento 24 horas entende ser necessário.

4.2 DESCRIÇÃO DO PROJETO

Este projeto consiste em um aplicativo móvel associado a um dispositivo de Internet das Coisas. O dispositivo IoT funciona como um alarme do local, possuindo um sensor de movimento que detecta a movimentação e irá informar no aplicativo um “alarme de invasão”, porém, na área controlada será silencioso, com o objetivo de ter tempo de ação de repressão e manter em segurança a vida dos envolvidos.

Este sistema possui, 3 modos de funcionamento que são: ativado, desativado e disparado. Para realizar as mudanças dos status do alarme, o dispositivo IoT possui sensor RFID que fará a leitura de cartões magnéticos - (TAG), onde somente as TAGs previamente cadastradas poderão realizar tais mudanças.

O aplicativo móvel fornece aos usuários informações como: invasões no perímetro e status atual do alarme. Também gera relatórios de acessos a reserva, de disparos do alarme, além de prover o gerenciamento de usuários. Foi desenvolvido para a plataforma Android, por ser o sistema operacional para smartphones mais utilizado atualmente e que possui maior facilidade na obtenção de informações técnicas para o desenvolvimento.

4.3 LEVANTAMENTO DE REQUISITOS

Nesta seção são apresentados os requisitos funcionais e não funcionais para o desenvolvimento, a partir da escolha e descrição do projeto.

4.3.1 Requisitos funcionais

Os requisitos funcionais fazem parte da funcionalidade do sistema, são processamentos necessários que geram os resultados esperados pelo cliente.

- **RF001** - Aplicar TAG no leitor RFID.

Descrição: Este requisito do sistema permite que o usuário altere o status do alarme, que varia do modo "Ativado" para o "Desativado" e vice-versa. Além disso, quando o alarme estiver no modo "Disparado", ao aplicar a TAG o status muda para o modo "Ativado".
Prioridade: Essencial.
Entradas e pré-condições: TAG estar previamente cadastrada no sistema.
Saídas e pós-condições: Status do alarme é alterado e o buzzer emite sinal sonoro.

- **RF002** - Cadastro.

Descrição: Permite ao novo usuário efetuar seu cadastro no sistema, obtendo assim, acesso a todas as funcionalidades do sistema.
Prioridade: Essencial.
Entradas e pré-condições: Token para cadastro, obtido previamente com o administrador do sistema.
Saídas e pós-condições: Usuário é cadastrado e direcionado para a tela principal do aplicativo.

- **RF003** - Login.

Descrição: Este requisito do sistema permite que o usuário efetue o login, tendo assim, acesso as funcionalidades do sistema.
Prioridade: Essencial.
Entradas e pré-condições: Usuário cadastrado no sistema.
Saídas e pós- condições: Usuário é direcionado para tela principal.

- **RF004** - Gerar Relatório.

Descrição: Permite ao usuário visualizar dados a respeito dos acessos e disparos do alarme no interior do depósito. Ambos os relatórios informarão a data, horário e status do alarme, mas apenas o relatório de acesso informará o código do cartão.
Prioridade: Importante.

Entradas e pré-condições: Seleção de data inicial e final para a geração do relatório.

Saídas e pós-condições: Visualização do relatório.

- **RF005** - Excluir Usuário.

Descrição: Este requisito permite ao administrador do sistema excluir um usuário cadastrado.

Prioridade: Essencial.

Entradas e pré-condições: Usuário com nível administrador.

Saídas e pós-condições: Usuário selecionado é excluído.

- **RF006** – Gerar Token.

Descrição: Permite ao administrador do sistema gerar um novo token para que um novo usuário se cadastre.

Prioridade: Essencial.

Entradas e pré-condições: Usuário que gera token deve possuir nível administrador, informar código do cartão e nível de permissão para o novo usuário.

Saídas e pós-condições: Novo token é gerado e informado.

- **RF007** – Detecta Movimento

Descrição: Este requisito do sistema permite que o usuário seja notificado via aplicativo, quando há detecção de movimento no interior do depósito quando o alarme se encontra no modo "Ativado".

Prioridade: Essencial.

Entradas e pré-condições: Status do alarme no modo "Ativado".

Saídas e pós-condições: Alteração do status do alarme para "Disparado" e envio de notificação via aplicativo.

4.3.2 Requisitos não-funcionais

Os requisitos não funcionais necessários ao sistema são listados aqui. Como a nomenclatura específica, estes requisitos não fazem parte da funcionalidade do sistema, mas são atributos essenciais para o bom funcionamento do sistema e influenciam em sua qualidade.

- **NF001** - Conectividade.

Descrição: O sistema precisa estar conectado à internet, tanto o dispositivo IoT quanto o aplicativo Android, para que seja realizada o envio e recebimento de dados.
Prioridade: Essencial.

- **NF002** - Segurança.

Descrição: Necessário para a segurança das informações. Sistema tem que restringir acesso de usuários não autorizados à informações sigilosas, proibir cadastro de usuários não autorizados e possuir criptografia de senha.
Prioridade: Essencial.

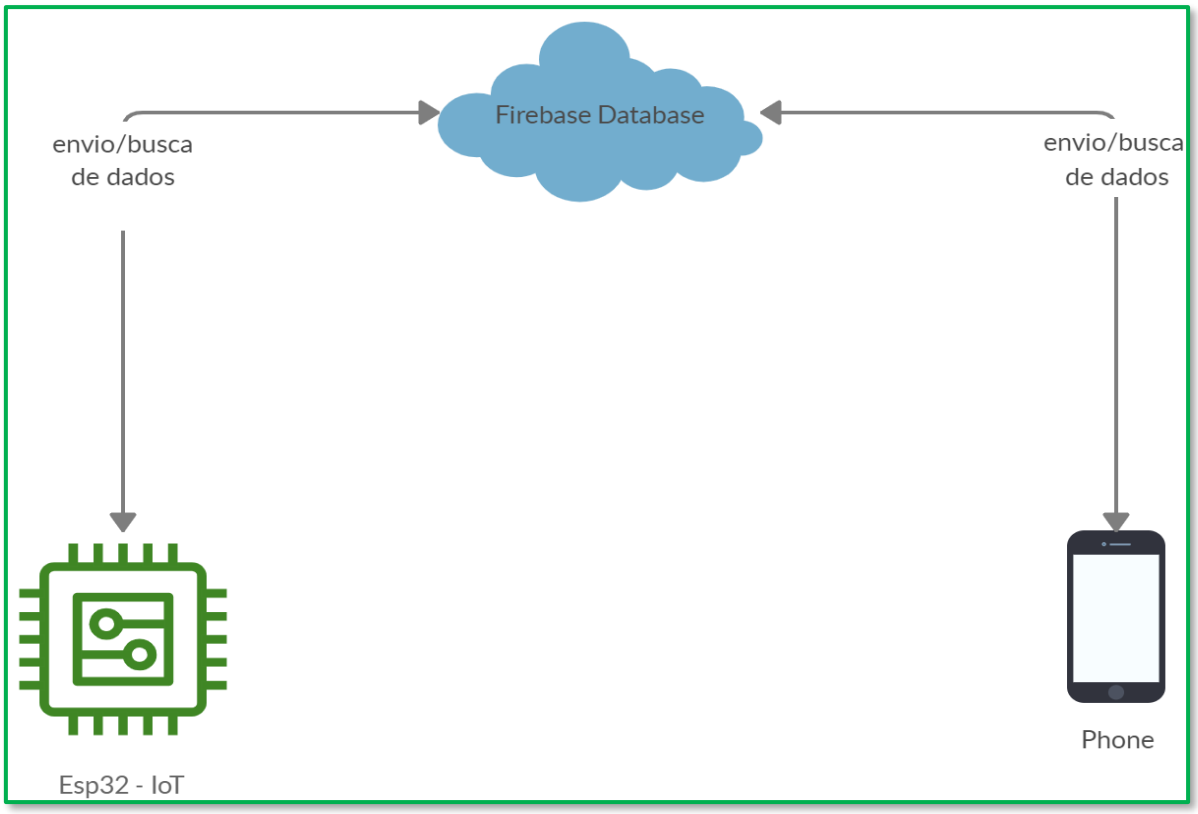
- **NF003** - Desempenho.

Descrição: É importante que o sistema tenha performance, sendo assim, a resposta aos processamentos seja eficaz e em tempo útil, para que a resposta humana física seja o mais breve possível.
Prioridade: Essencial.

4.4 IMPLEMENTAÇÃO

Inicialmente foi projetada a comunicação entre o dispositivo IoT e o aplicativo móvel, tomando por base um princípio, o armazenamento de dados não poderia ser local, precisaria de conexão com a internet para que os dados pudessem ser atualizados em tempo real para todos os usuários. Logo chegou-se à conclusão de que o dispositivo IoT faria o envio e busca de dados, assim como o aplicativo móvel também, portanto a comunicação poderia ser feita através de um banco de dados na nuvem. Decidiu-se então utilizar o Firebase pela facilidade de implementação no projeto, além de não possuir custo. Na Figura 11, segue diagrama para exemplificar a comunicação:

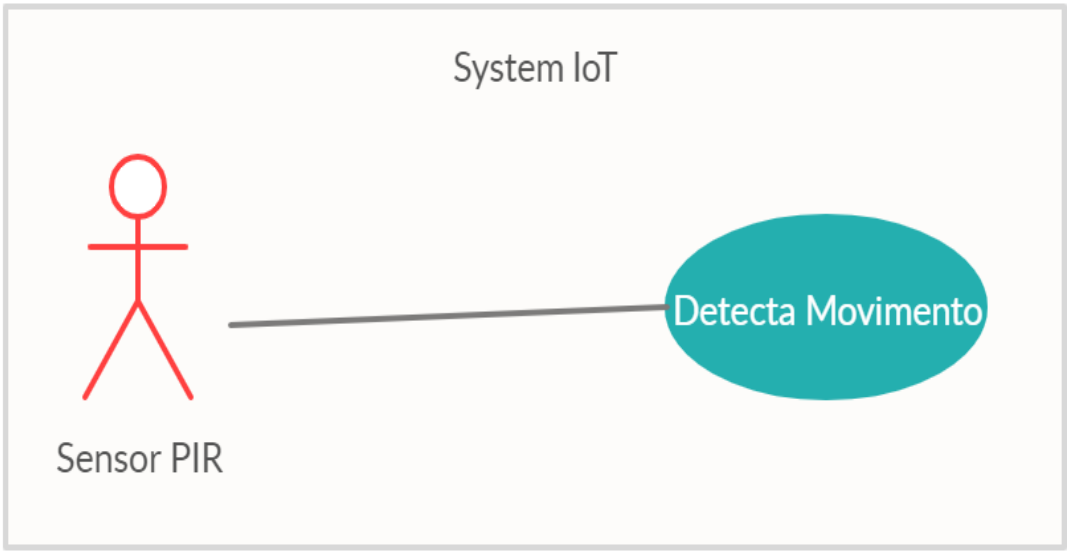
Figura 11. Diagrama comunicação.



Fonte: Desenvolvido pelo autor.

O sistema possui um total de 7 casos de uso. O primeiro é o caso de uso “Detecta Movimento”, com seu diagrama apresentado na Figura 12.

Figura 12. Diagrama de caso de uso “Detecta Movimento”.



Fonte: Desenvolvido pelo autor.

- **Nome do Caso de Uso:** Detecta Movimento.
- **Descrição:** Este caso de uso se inicia quando o sensor PIR identifica movimento.
- **Eventos:** Sensor PIR identifica movimento.
- **Atores:** Sensor PIR.
- **Pré-condições:** Status do alarme ativo.
- **Pós-Condições**
    - **Conclusões com sucesso**
        - Envio de notificação de disparo do alarme para os usuários do sistema.
        - Alteração do status do alarme.
    - **Conclusões sem sucesso**
        - Não é enviada notificação de disparo.
        - Status do alarme não é alterado.
- **Fluxo básico**
    - Sensor PIR identifica movimento.
    - Alteração do status para “Alarme Disparado”.
    - Envio de notificação.

Desenvolveu-se a codificação para que a leitura de movimento seja feita conforme o status do alarme, então primeiramente o sistema verifica o status atual do alarme, sendo eles: ativado, desativado e disparado.

No modo ativado o sensor de movimento fica ativo para a detecção de radiação infravermelha dentro de seu campo de atuação. Quando identificado o movimento pelo sensor, é alterado o status do alarme para disparado e em seguida é enviada uma notificação no aplicativo conforme a Figura 13.

Figura 13. Notificação.

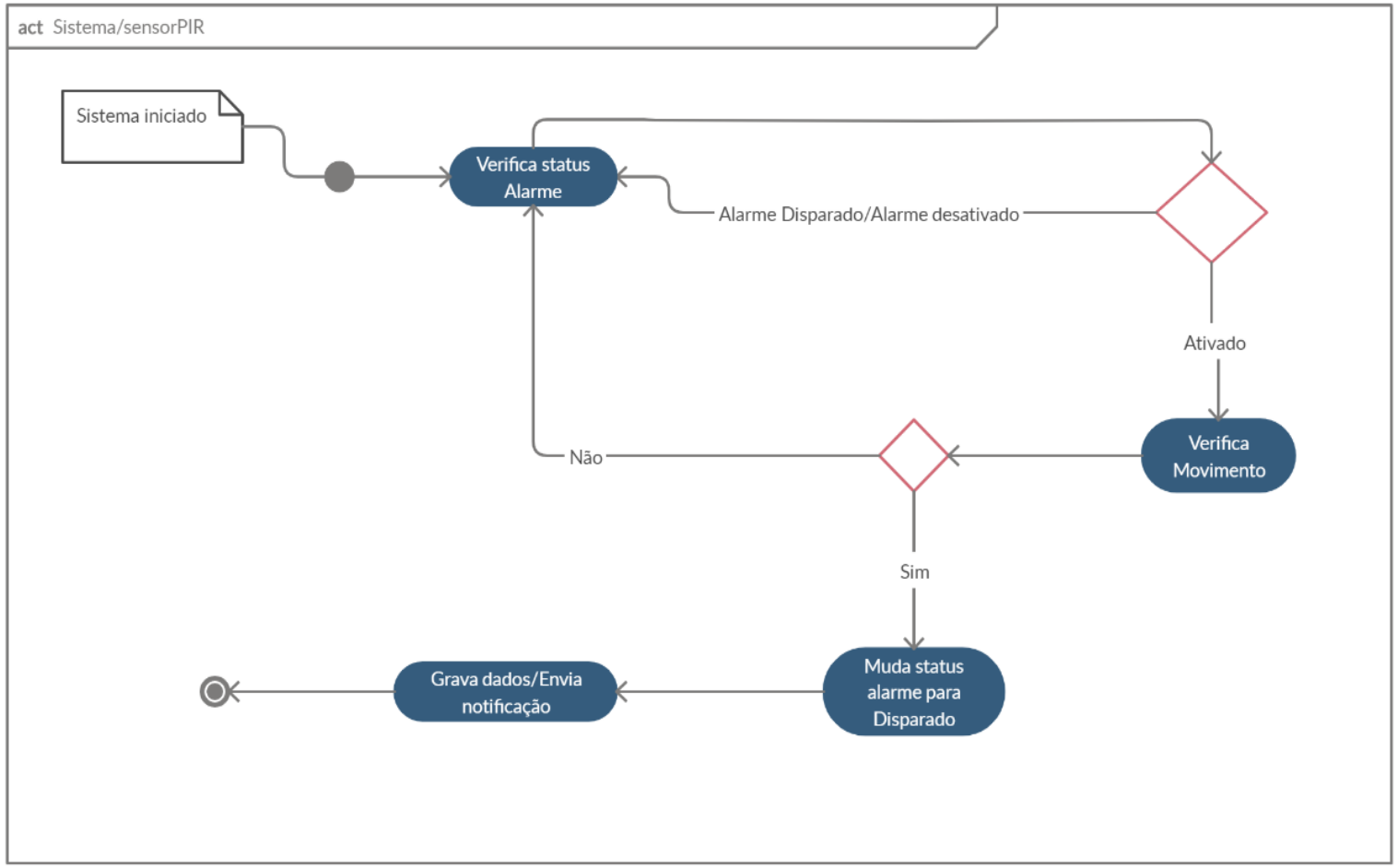
Fonte: Desenvolvido pelo autor.

O alarme não emite alerta sonoro, pois o objetivo com esta notificação é proteger a vida dos envolvidos. Com este aviso, todos os responsáveis pela reserva seriam notificados através do smartphone, mesmo não estando

escalados para a guarda, isso possibilita que os policiais possam intervir no caso de invasão ao local e rendição de furriéis por parte de criminosos. Para trazer melhor entendimento, caso o alarme emitisse som, os criminosos no momento da abordagem aos furriéis, seriam alertados, sendo assim, haveria maior probabilidade do uso de violência contra os policiais. Além disso, compreenderiam que o reforço policial estaria a caminho, dificultando a sua captura.

No modo desativado, como o próprio nome sugere, o sensor não atua. Por último, o modo disparado é o estado logo após a identificação de movimento no status ativado. Na Figura 14 é apresentado o diagrama de atividade do caso de uso “Detecta Movimento”.

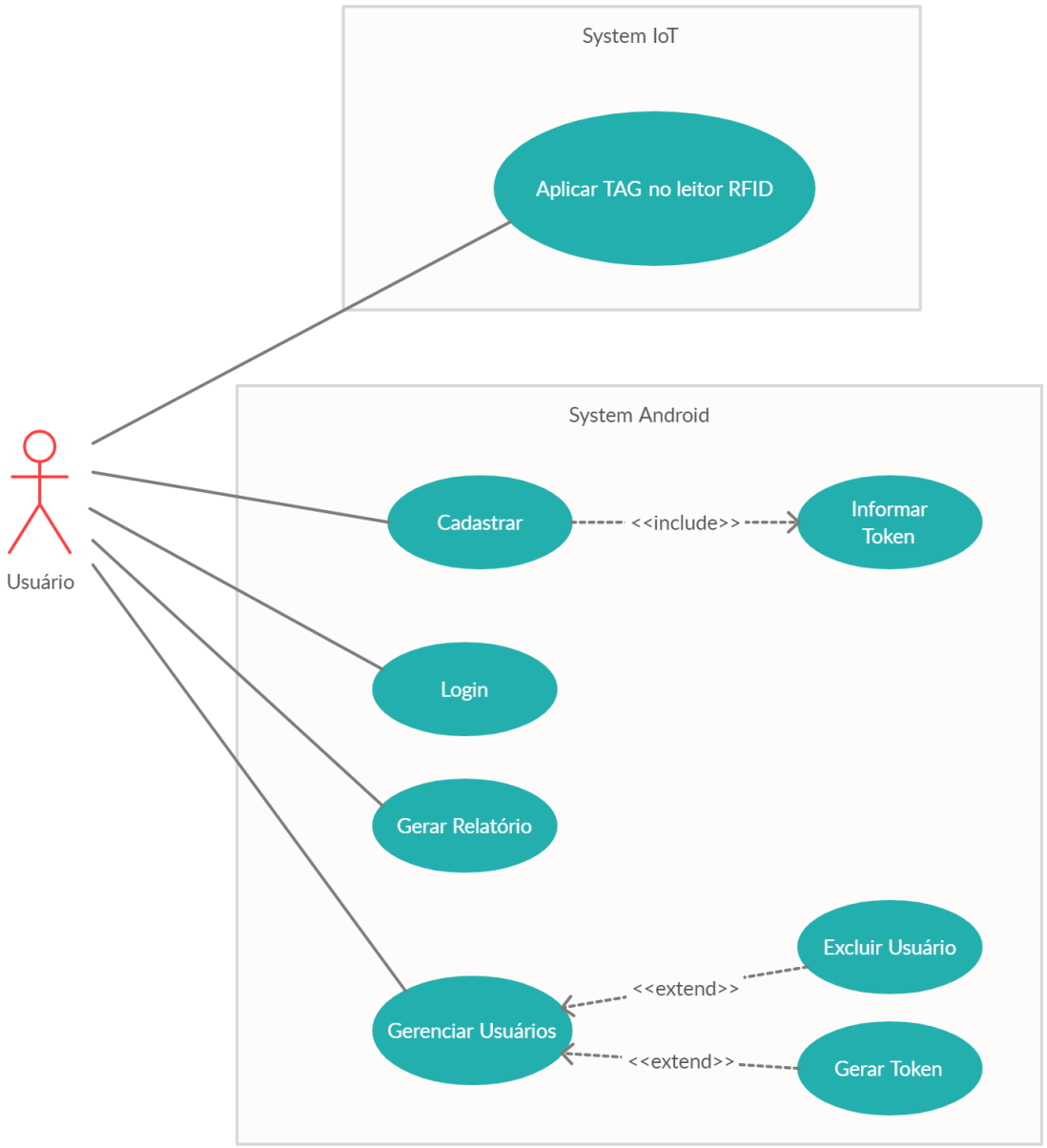
Figura 14. Diagrama de atividade do caso de uso “Detecta Movimento”.



Fonte: Desenvolvido pelo autor.

Na Figura 15, temos o diagrama de casos de uso do usuário com o dispositivo IoT e com o aplicativo móvel.

Figura 15. Diagrama de caso de uso do usuário com dispositivo IoT e com aplicativo móvel.



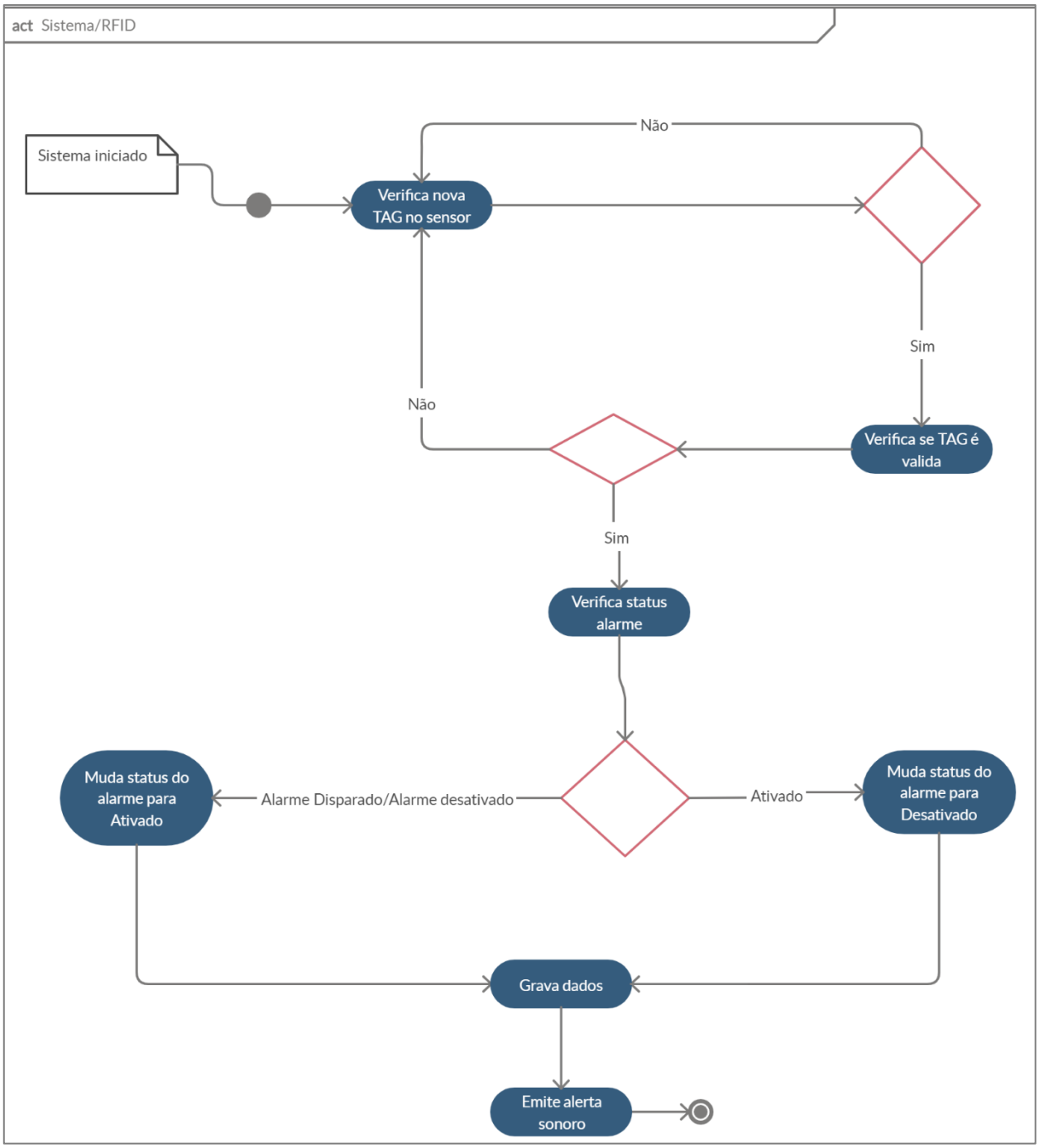
Fonte: Desenvolvido pelo autor.

O único caso de uso do usuário com o dispositivo IoT é a aplicação do TAG, segue descrição do caso de uso.

- **Nome do Caso de Uso:** Aplicar TAG no leitor RFID.
- **Descrição:** Este caso de uso se inicia quando o usuário aplica a TAG no leitor de RFID do dispositivo IoT.
- **Eventos**
    - Leitura da TAG.
    - Validação da TAG.
- **Atores:** Usuário.
- **Pré-condições:** Usuário possuir uma TAG cadastrada.
- **Pós-Condições**
    - **Conclusões com sucesso:** Alteração do status do alarme.
    - **Conclusões sem sucesso:** Status do alarme não é alterado.
- **Fluxo básico**
        - Usuário passa a TAG no leitor.
        - RFID faz a leitura da TAG.
        - Validação da TAG (A1).
        - TAG é autorizado.
        - Status do alarme é alterado(B1).
        - Emissão de aviso sonoro.
- **Fluxos alternativos**
        - A1: em "3. Validação da TAG", se for autorizada vai para item 4, se não A1.1.
        - A1.1: Status atual do alarme permanece sem alteração.
        - B1: em “5. Status do alarme é alterado”, se status atual for “desativado” ou “Alarme Disparado” muda para “Ativado”, se não B1.1.
        - B1.1: Status atual do alarme muda para “desativado”.

Na Figura 16 é apresentado o diagrama de atividade do caso de uso “Aplicar TAG no leitor RFID”.

Figura 16. Diagrama de atividade do caso de uso “Aplicar TAG no leitor RFID”.

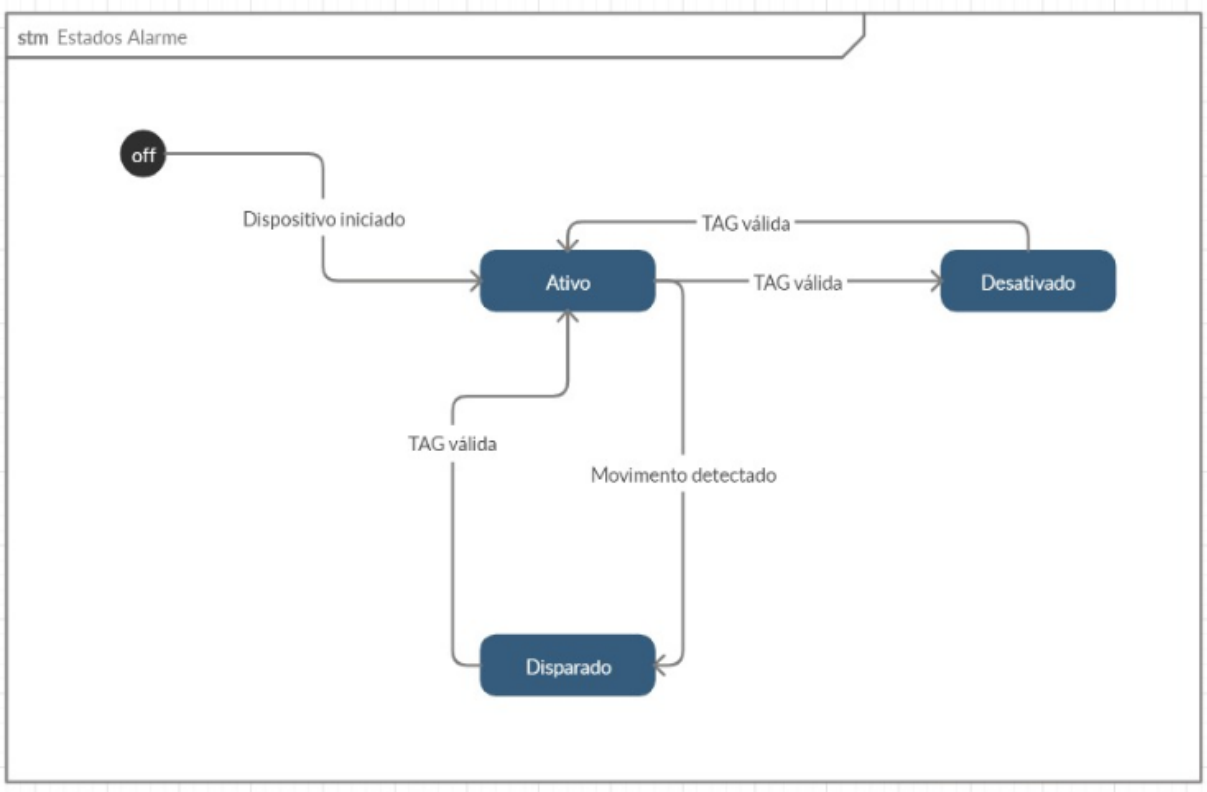


Fonte: Desenvolvido pelo autor.

Pode-se observar que o sistema sempre está verificando a presença de uma nova TAG no sensor, sendo verdadeira, o sistema verifica a sua validade, pois necessita estar previamente cadastrada. Portanto, a TAG estando

autorizada ocorre a mudança no status, conforme o diagrama de estados do alarme representado na Figura 17.

Figura 17. Diagrama de estados do alarme.



Fonte: Desenvolvido pelo autor.

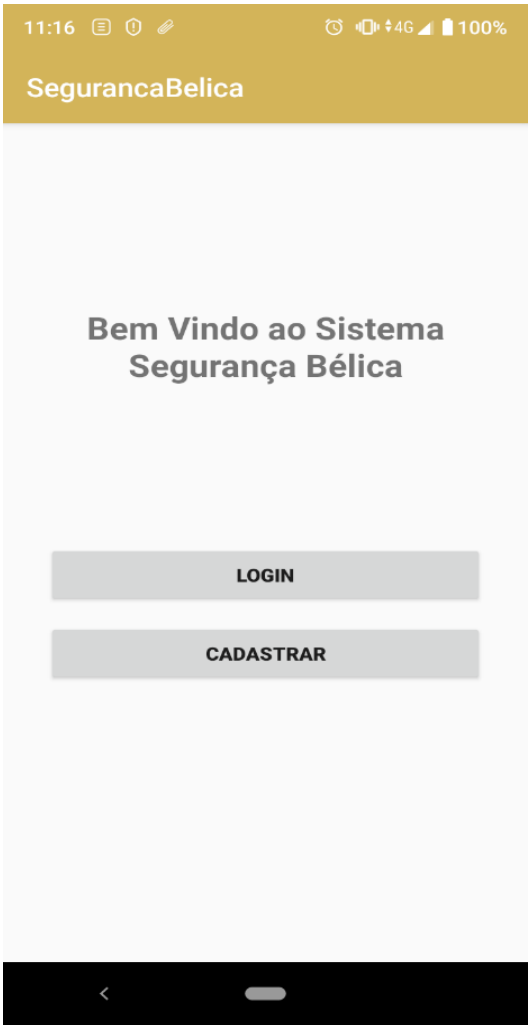
O próximo caso de uso é o cadastro do usuário, exigirá obrigatoriamente que o usuário possua um número de token fornecido pelo administrador do sistema (caso de uso “token”, será explicado na sequência).

- **Nome do Caso de Uso:** Cadastrar.
- **Descrição:** Este caso de uso se inicia quando usuário abre o aplicativo segurança bélica.
- **Eventos:** Usuário realiza o cadastro.
- **Atores:** Usuário.
- **Pré-condições:**
    - Aplicativo Segurança Bélica instalado.
    - Aplicativo na tela inicial.
    - Usuário possuir token para cadastro.

- **Pós-Condições:**
  - **Conclusões com sucesso:** Usuário é cadastrado.
  - **Conclusões sem sucesso:** Usuário não é cadastrado.
- **Fluxo básico:**
    - Usuário clica em “Cadastrar”.
    - Usuário preenche os campos.
    - Clica em “Cadastrar”.
    - Verificação dos dados (A1).
    - Direciona para tela principal do aplicativo.
- **Fluxos alternativos:**
    - A1: em "4. Verificação dos dados", se estão os campos “nome”, “posto”, “token”, “e-mail” e “senha” preenchidos corretamente segue para o item 4, se não A1.1
    - A1.1. Informa o usuário sobre quais dados estão incorretos.

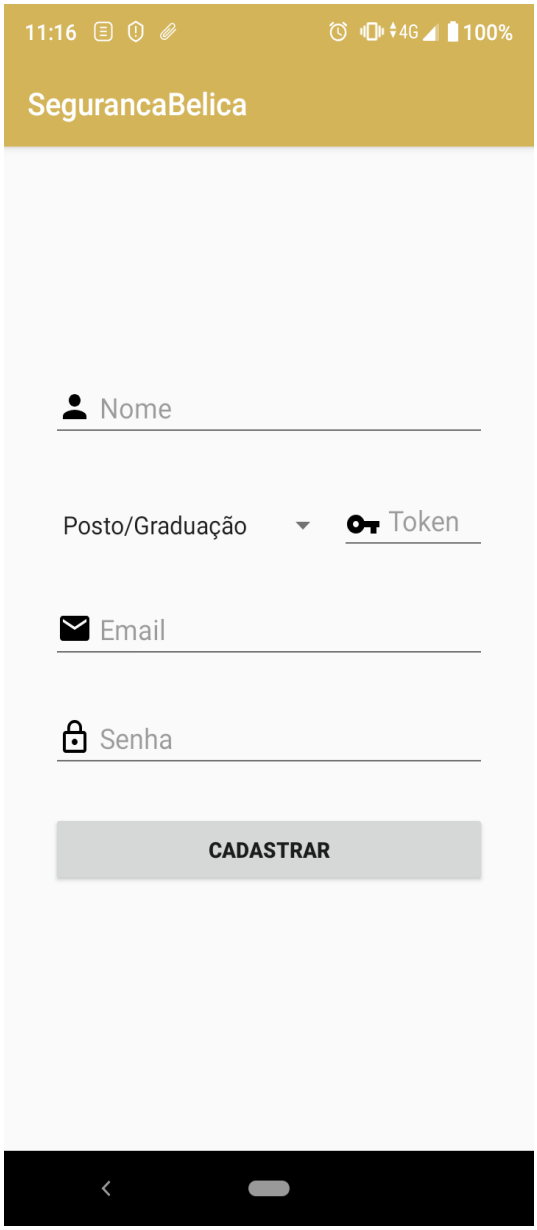
Este caso de uso gera duas telas, que serão demonstradas através das Figuras 18 e 19.

Figura 18. Tela Inicial do aplicativo.



Fonte: Desenvolvido pelo autor.

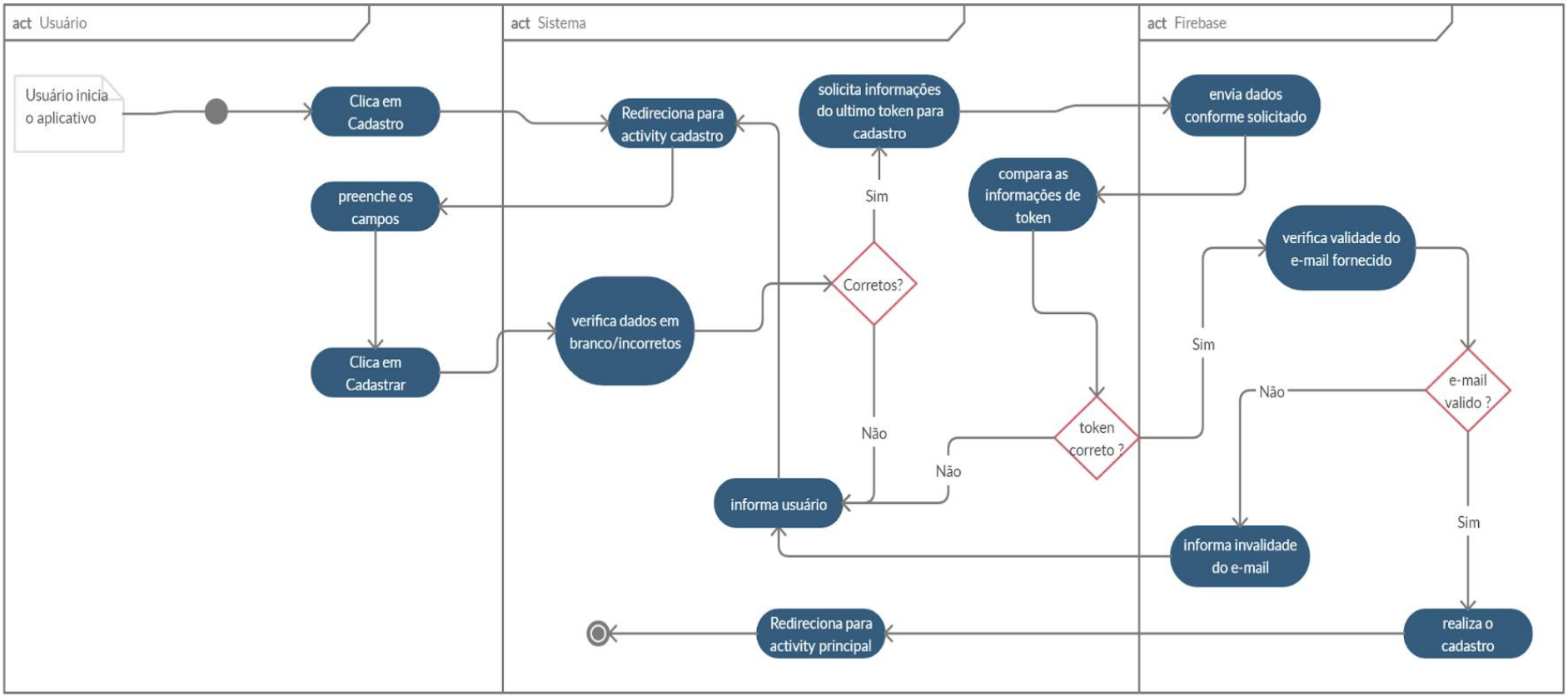
Figura 19. Tela de cadastro.



Fonte: Desenvolvido pelo autor.

Após o preenchimento correto, o sistema solicita informações do último token para o Firebase, após resposta, realiza as comparações necessárias e então envia os dados para cadastro ao banco de dados. Este realiza mais verificações a respeito do e-mail e então retorna a resposta para o sistema dar prosseguimento. A seguir o diagrama de atividade do caso de uso “Cadastrar”, apresentado na Figura 20, complementa a explicação do que foi desenvolvido.

Figura 20. Diagrama de atividade do caso de uso “Cadastrar”.

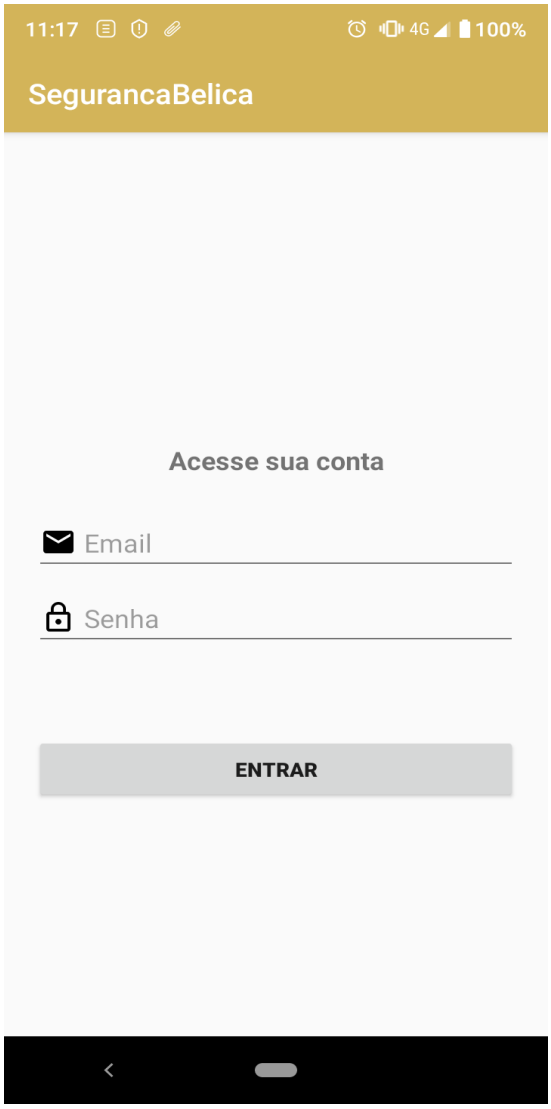


Fonte: Desenvolvido pelo autor.

O caso de uso a seguir é a realização do login pelo usuário, é necessário que possua cadastro no sistema.

- **Nome do Caso de Uso:** Login.
- **Descrição:** Usuário realiza o login no aplicativo.
- **Eventos:** Usuário loga no aplicativo.
- **Atores:** Usuário.
- **Pré-condições:**
    - Usuário cadastrado no sistema.
    - Aplicativo na tela inicial.
- **Pós-Condições:**
    - **Conclusões com sucesso:** Usuário é direcionado para tela principal.
    - **Conclusões sem sucesso:** Usuário não é direcionado para tela principal.
- **Fluxo básico:**
    - Usuário clica em “Login”.
    - Preenche os campos.
    - Clica em “Entrar”.
    - Verificação dos dados (A1).
    - Direciona para tela principal do aplicativo.
- **Fluxos alternativos:**
    - A1: em "4. Verificação dos dados", se estão os campos “e-mail” e “senha” preenchidos corretamente segue para o item 5, se não A1.1.
    - A1.1. Informa o usuário sobre quais dados estão incorretos.

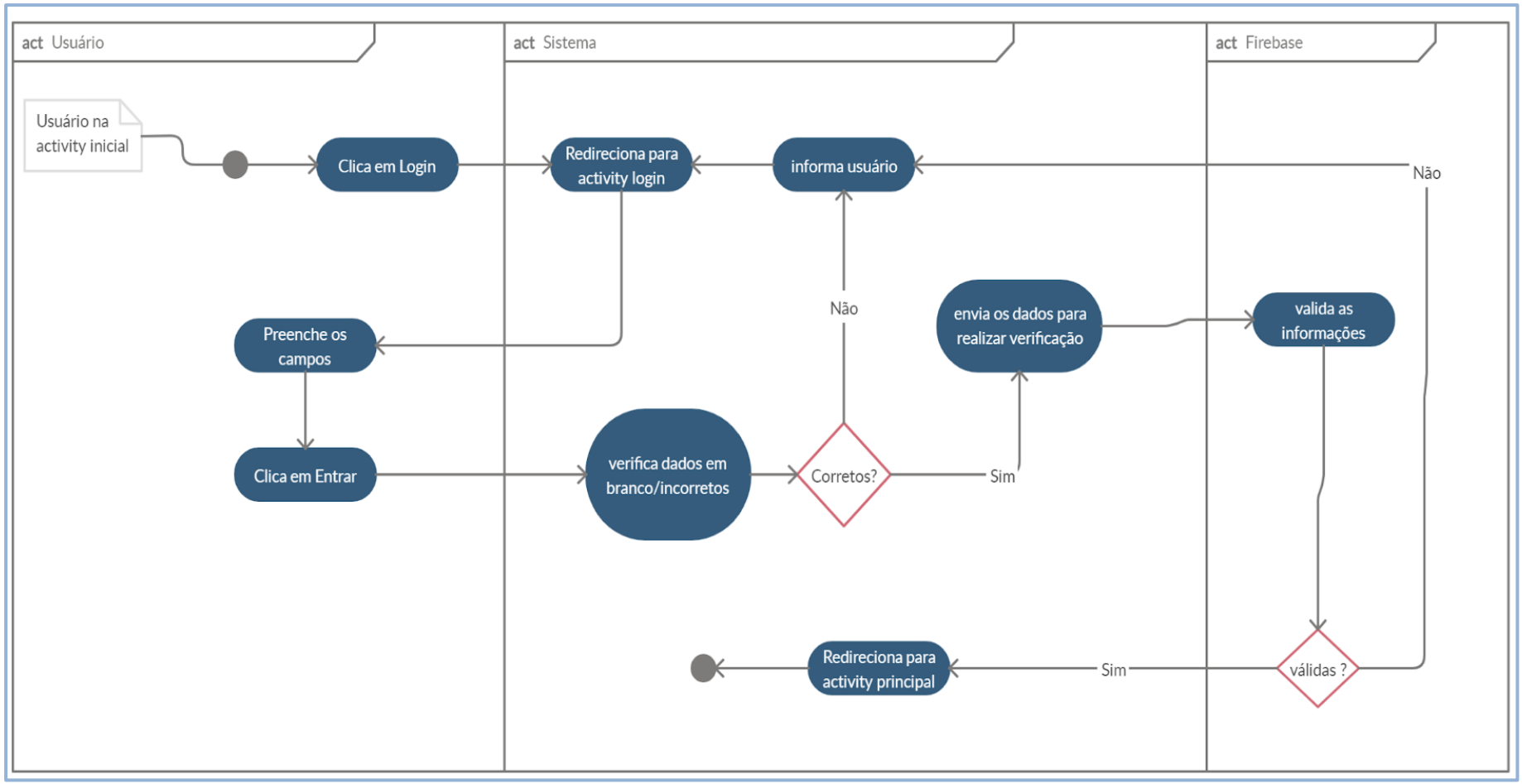
Figura 21. Tela do login.



Fonte: Desenvolvido pelo autor.

Após inserção dos dados o sistema realiza uma verificação inicial, estando válidos então os envia ao Firebase para que faça a verificação da veracidade dos dados, após isso é retornado a resposta e seu encaminhamento. O diagrama de atividade do caso de uso “Login” na Figura 22, apresenta o que foi desenvolvido.

Figura 22. Diagrama de atividade do caso de uso “Login”.



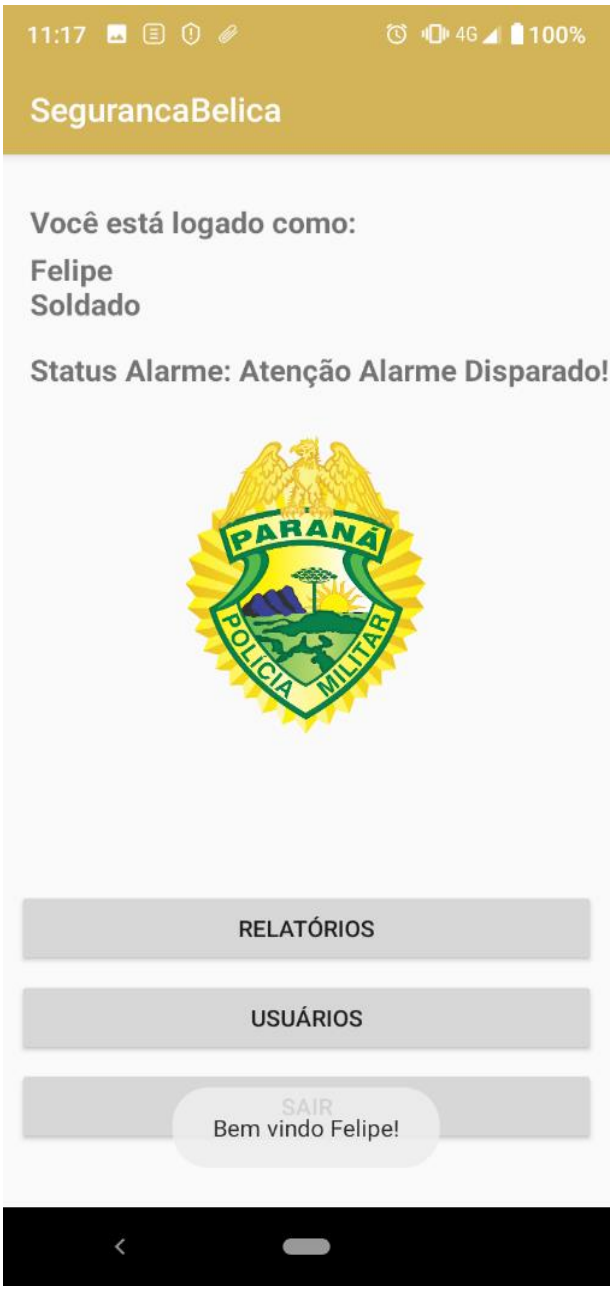
Fonte: Desenvolvido pelo autor.

O caso de uso a seguir é a geração de relatórios a respeito dos acessos e dos disparos do alarme, abaixo a descrição.

- **Nome do Caso de Uso:** Gerar Relatório.
- **Descrição:** Geração de relatório pelo sistema.
- **Eventos:**
    - Sistema gera relatório de acessos.
    - Sistema gera relatório de disparos de alarme.
- **Atores:**
    - Usuário.
    - Sistema.
- **Pré-condições:**
    - Usuário logado no sistema.
    - Aplicativo na tela principal do sistema.
- **Pós-Condições:**
    - **Conclusões com sucesso:** Sistema gera relatório.
    - **Conclusões sem sucesso:** Sistema não gera relatório.
- **Fluxo básico:**
    - Usuário clica em “Relatório”.
    - Preenche data inicial e final.
    - Clica em “Gerar Relatório Acesso” ou “Gerar Relatório Disparo Alarme”.
    - Sistema realiza a busca dos dados (A1).
    - É apresentado ao usuário uma lista com os dados.
- **Fluxos alternativos:**
    - A1: em "4. Sistema realiza a busca dos dados ", se encontrar dados segue para item 5, se não A1.1.
    - A1.1. Informa ao usuário que não existem dados.

O caso de uso acontecerá nas seguintes telas do aplicativo, apresentado nas Figuras 23, 24, 25, 26, 27 e 28.

Figura 23. Tela menu principal.



Fonte: Desenvolvido pelo autor.

Figura 24. Tela de relatórios

Fonte: Desenvolvido pelo autor.

Após ser selecionado o botão “relatórios” contido na tela da Figura 23, será direcionado para os relatórios, representado na Figura 24. Nessa tela deve ser selecionada a data inicial e final, conforme botões representados nessa figura.

A seguir a Figura 25, mostra como o usuário pode realizar a seleção da data inicial, conforme o prazo de tempo que deseja visualizar o resultado do relatório.

Figura 25. Tela escolha da data inicial.

Fonte: Desenvolvido pelo autor.

A seguir a Figura 26, mostra como o usuário pode realizar a seleção da data final, assim delimita o prazo do relatório.

Figura 26. Tela data final.

Fonte: Desenvolvido pelo autor.

Figura 27. Tela relatório de acesso.

Fonte: Desenvolvido pelo autor.

Após o usuário clicar no botão “Gerar relatório de acesso”, conforme a Figura 27, será possível visualizar os dados referente ao prazo anteriormente estipulado, então a tela de relatórios será gerada com as informações de status do alarme, códigos de cartão, data e hora. Viabiliza a análise para usuário, dos períodos em que o alarme foi ativado e desativado, como também informa quem foram os agentes que alteraram esse status, através dos códigos. Neste

momento já é possível ter uma gestão do fluxo de acesso às áreas de armamento.

Figura 28. Tela relatório de disparos.

Fonte: Desenvolvido pelo autor.

Após selecionar o botão “Gerar relatórios disparos alarme”, a tela gera, conforme apresentado na Figura 28, os registros sobre o status do alarme, data e hora em que identificou acessos sem permissão na área monitorada.

Para a geração do relatório foi necessário que o envio de dados ao Firebase, a partir do dispositivo IoT, fosse realizada à duas tabelas distintas, uma para os acessos com a TAG e outra para os disparos do alarme. Ocorrendo a passagem da TAG no sensor RFID ou a detecção de movimento pelo sensor PIR, o dispositivo IoT busca os dados de data e hora atuais na rede, transforma-os no tipo inteiro, então com esses dados, monta o tipo JSON "Javascript Object Notation" para enviar ao Firebase. No banco de dados as informações finais são gravadas conforme as Figuras 29 e 30.

Figura 29. Objeto acessos.

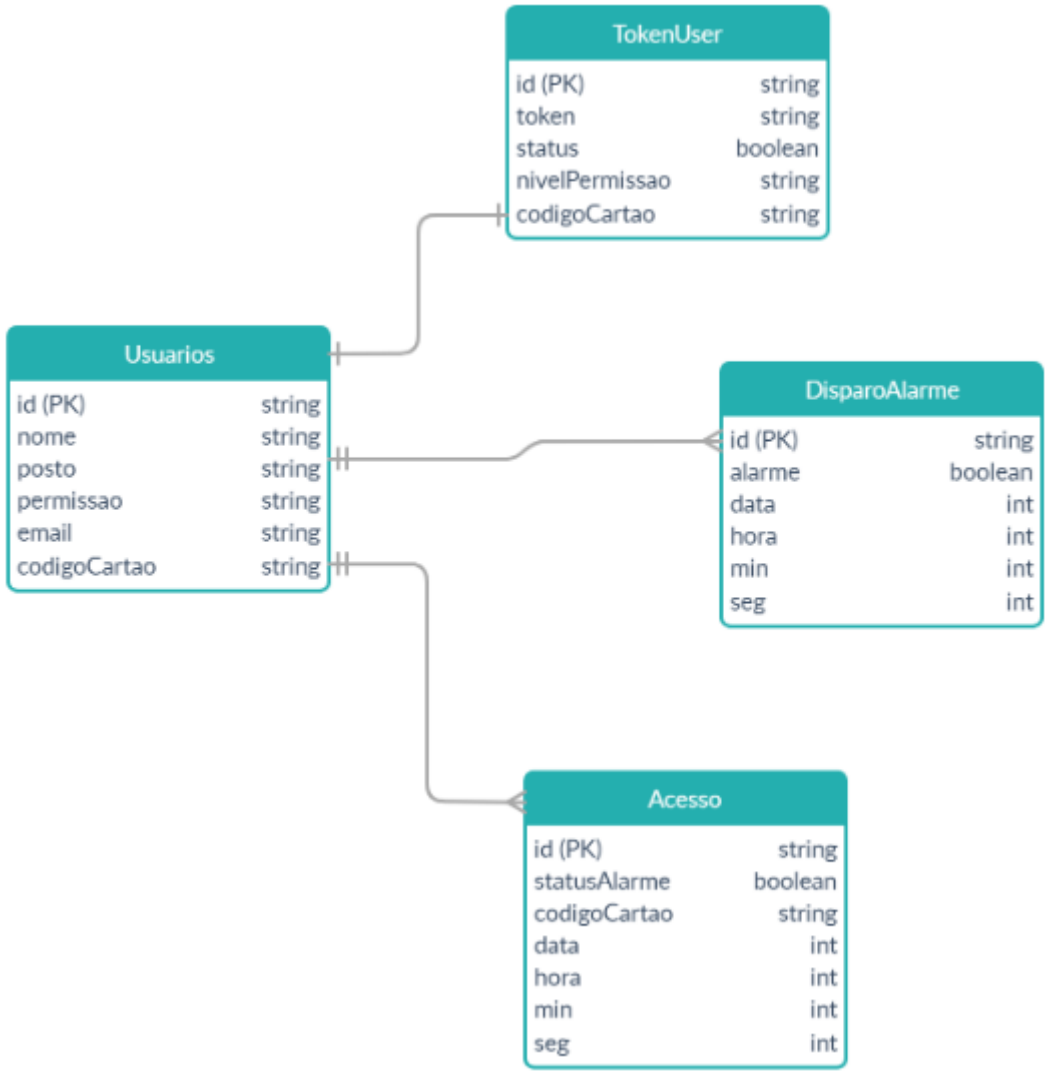
Fonte: Desenvolvido pelo autor.

Figura 30. Objeto disparo alarme.

Fonte: Desenvolvido pelo autor.

A Figura 31 apresenta o diagrama do banco de dados que contém todas as informações que são buscadas e gravadas tanto pelo aplicativo, quanto pelo dispositivo IoT.

Figura 31. Diagrama do banco de dados.

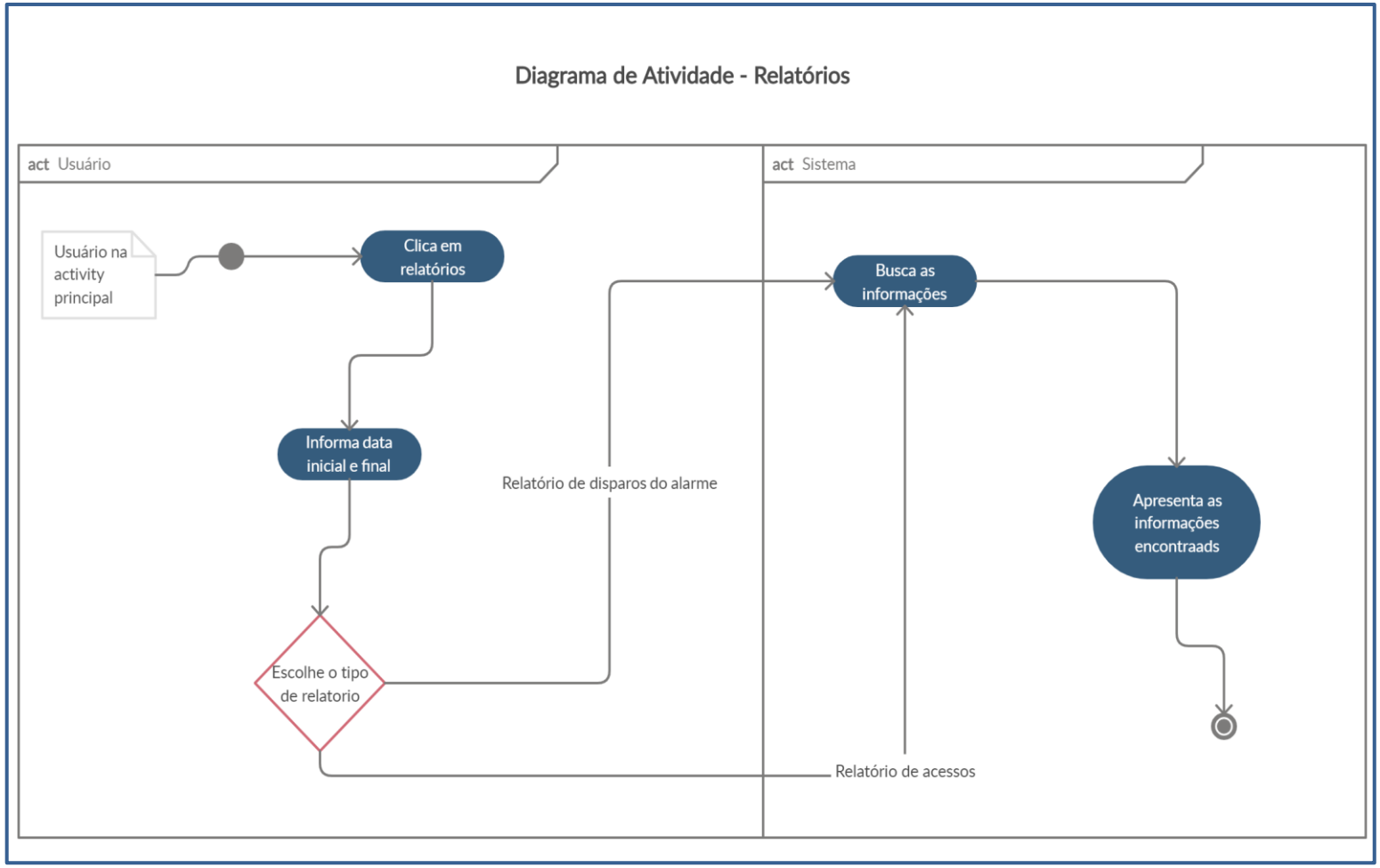


Fonte: Desenvolvido pelo autor.

A data precisou ficar em ordem invertida, por exemplo a data: “10-02-2020”, além de transformada para o tipo inteiro como dito anteriormente, foi também formatada para “20200210” isso ocorreu devido ao fato do Firebase não possuir um método específico para busca de intervalos de datas, portanto a busca foi feita a partir do método “`.orderByChild("data"). startAt(dataInicio). endAt(dataFim);`” que busca um intervalo de dados entre um número inteiro até outro.

O diagrama de atividade do caso de uso “Gerar Relatório” na Figura 32, mostra o ciclo completo.

Figura 32. Diagrama de atividade do caso de uso “Gerar Relatório”.



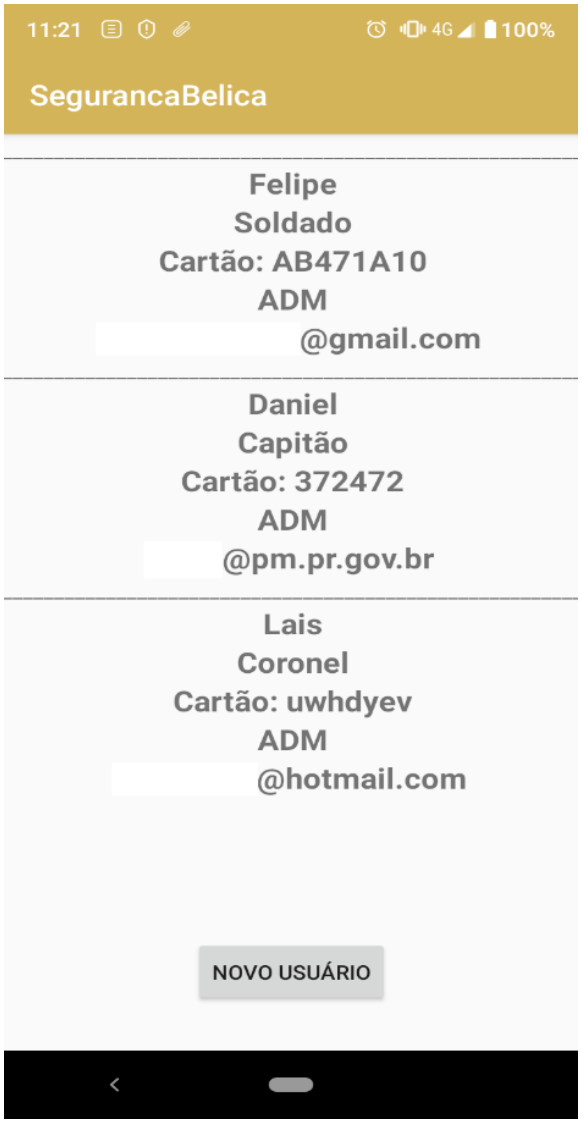
Fonte: Desenvolvido pelo autor

A seguir é descrito o caso de uso para exclusão de usuário que faz parte do gerenciamento de usuários de um modo geral.

- **Nome do Caso de Uso:** Excluir Usuário
- **Descrição:** Exclusão de usuário do sistema.
- **Eventos:** Usuário administrador exclui outro usuário do sistema.
- **Atores:** Usuário administrador.
- **Pré-condições:**
    - Usuário com nível administrador.
    - Aplicativo na tela principal do sistema.
- **Pós-Condições:**
    - **Conclusões com sucesso:** Usuário selecionado é excluído.
    - **Conclusões sem sucesso:** Não exclui usuário.
- **Fluxo básico:**
    - Usuário clica em “Usuários”.
    - Direcionamento para tela lista de usuários.
    - Usuário seleciona item deslizando na tela sentido esquerda para direita.
    - Mensagem de confirmação é apresentada (A1).
    - Usuário selecionado é excluído.
- **Fluxos alternativos**
    - A1: em "4. Mensagem de confirmação é apresentada", se usuário clicar em “Confirmar” segue para item 5, se não A1.1.
    - A1.1. Informa o usuário que a operação foi cancelada.

As telas desse caso de uso são apresentadas nas Figuras 33 e 34.

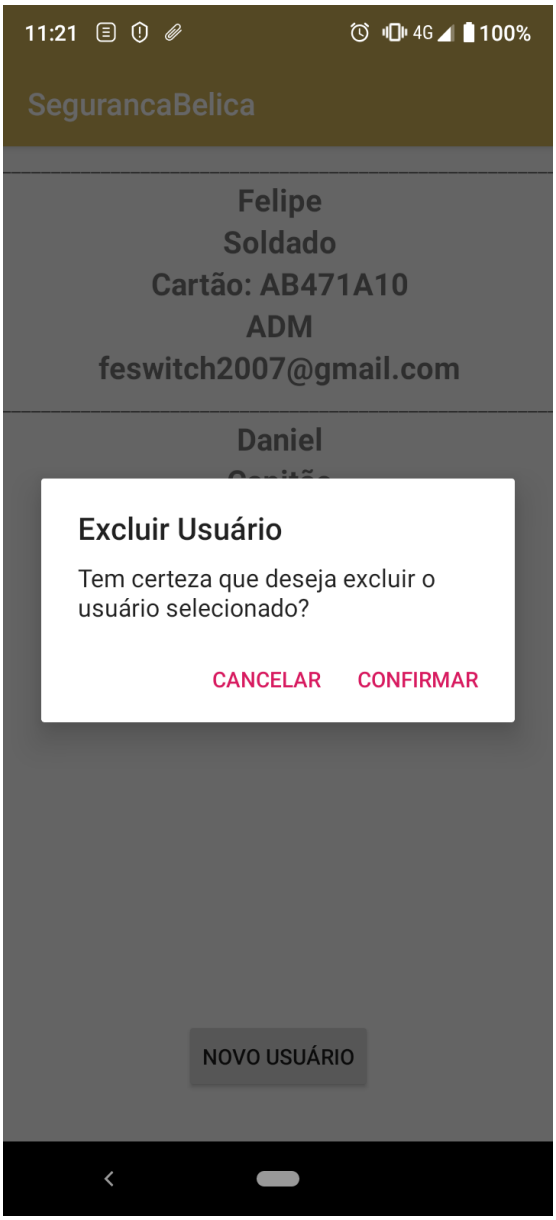
Figura 33. Tela lista de usuários.



Fonte: Desenvolvido pelo autor.

Nessa tela o usuário pode visualizar as informações: nome, posto, código do cartão e e-mail. Dependendo do nível de permissão de acesso ao sistema, os dados estarão disponíveis. Um exemplo é que o superior direto poderá enxergar todas as informações e o furriel não terá acesso à esta tela.

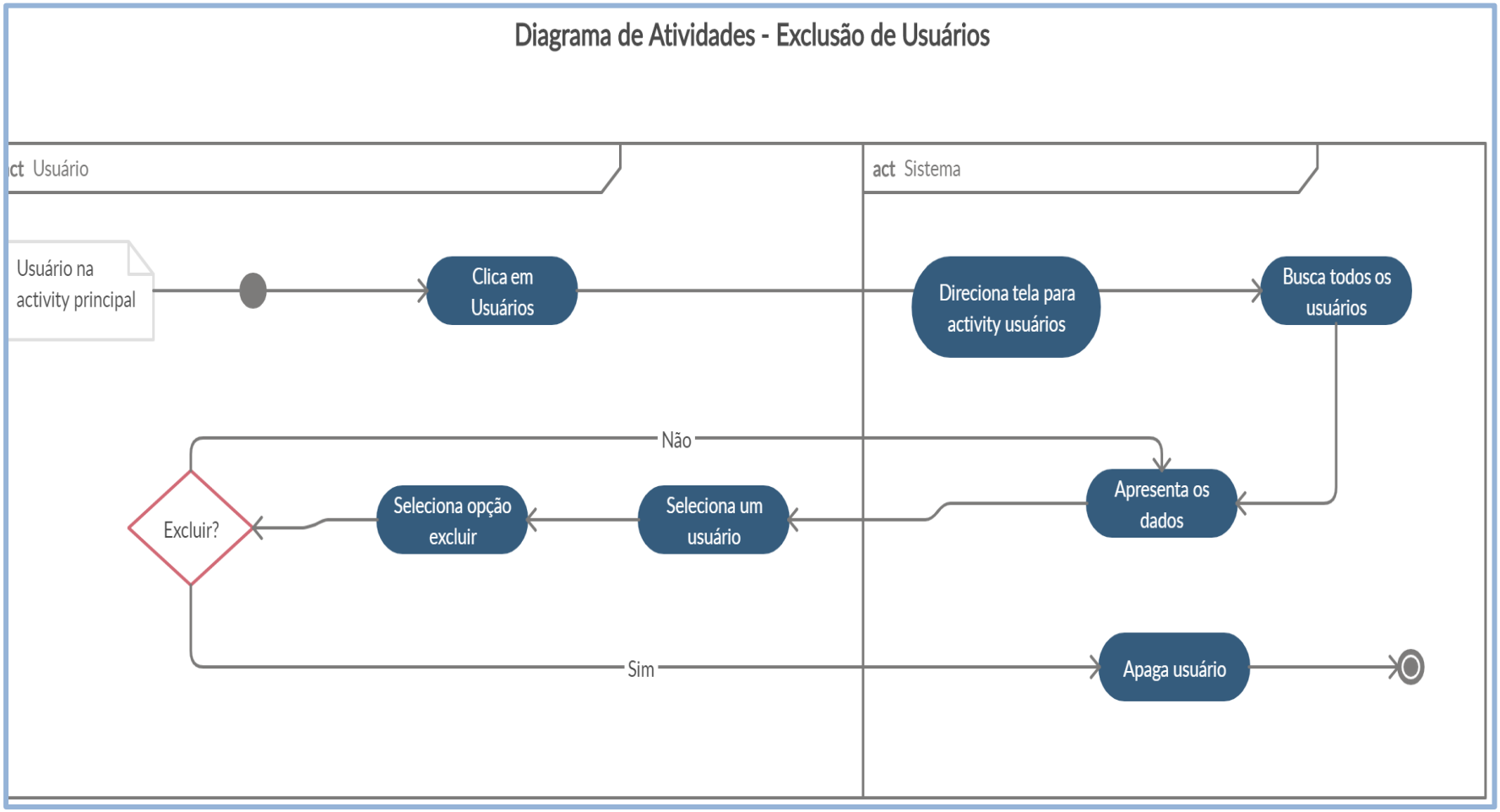
Figura 34. Tela confirmação de exclusão.



Fonte: Desenvolvido pelo autor.

Após a seleção do usuário, o sistema cria um “AlertDialog”, conforme Figura 34, para que o usuário confirme ou cancele a operação, selecionando confirmar o sistema realiza a exclusão, caso contrário a operação não será efetivada. Na Figura 35 é apresentado o diagrama de atividade do caso de uso “Excluir Usuário” complementando o que foi desenvolvido.

Figura 35. Diagrama de atividade do caso de uso “Excluir Usuário”.



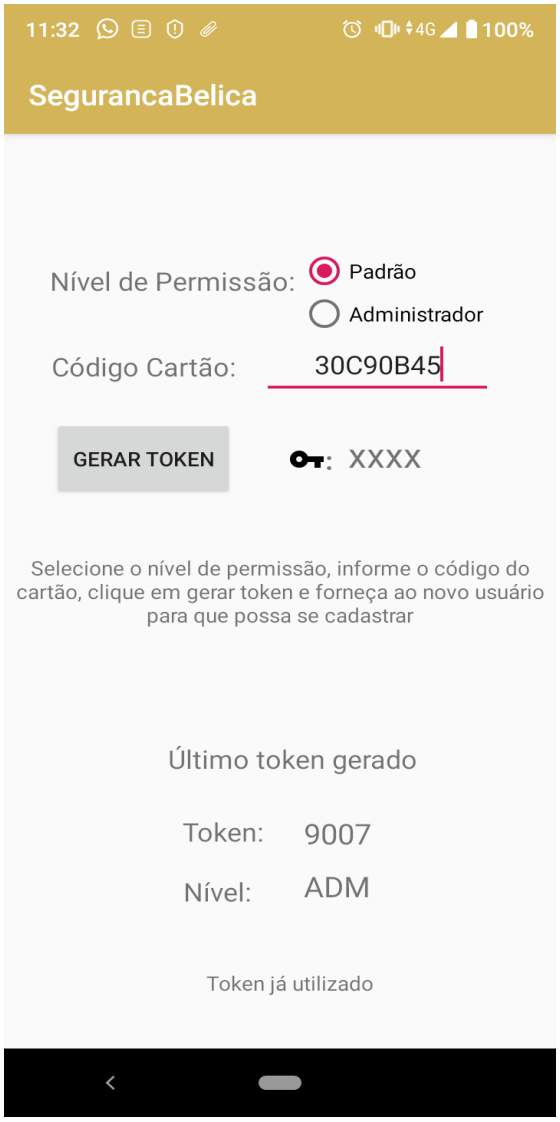
Fonte: Desenvolvido pelo autor.

Por fim, o último caso de uso é a geração do token para cadastro de novos usuários, esse faz parte do gerenciamento de usuários.

- **Nome do Caso de Uso:** Gerar Token
- **Descrição:** Usuário solicita geração de token para cadastro de novo usuário no sistema.
- **Eventos:** Sistema gera token.
- **Atores:**
    - Usuário.
    - Sistema.
- **Pré-condições:**
    - Usuário com nível administrador.
    - Aplicativo na tela de lista de usuários.
- **Pós-Condições:**
    - **Conclusões com sucesso:** Novo token é gerado.
    - **Conclusões sem sucesso:** Token não é gerado.
- **Fluxo básico:**
    - Usuário clica em “Novo Usuário”.
    - Direciona para tela de token.
    - Usuário preenche os dados.
    - Clica em “Gerar Token”.
    - Token é gerado e apresentado na tela.

As telas do aplicativo na geração do token, são apresentadas nas Figuras 36 e 37.

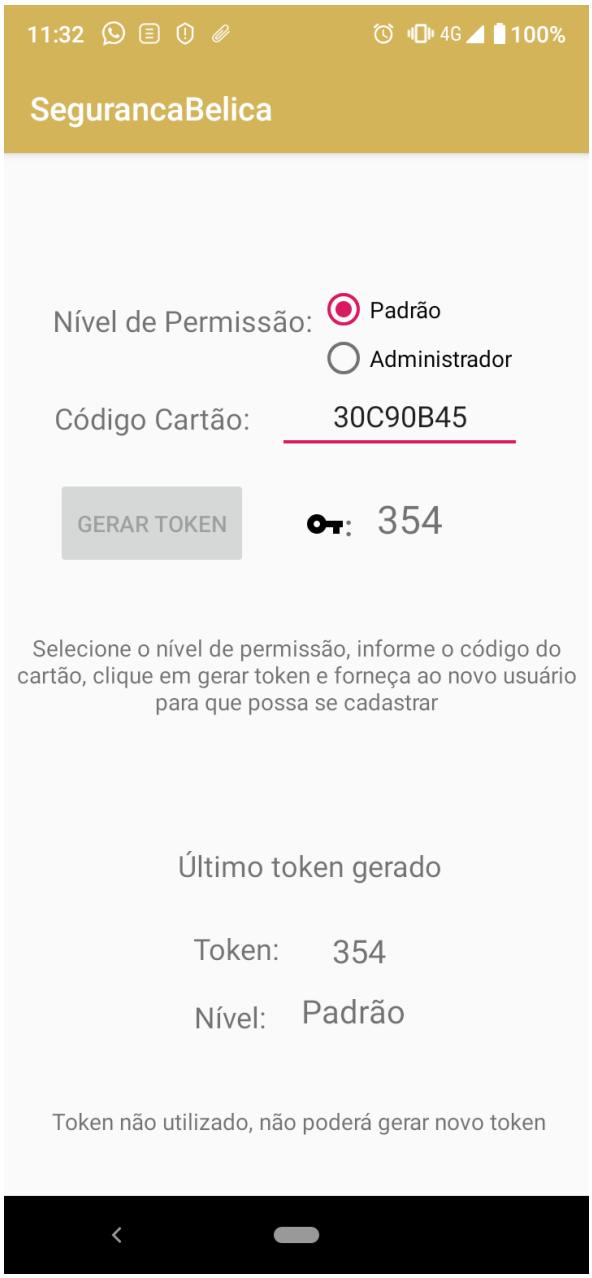
Figura 36. Tela gerar token.



Fonte: Desenvolvido pelo autor.

Conforme a Figura 36 o usuário deve selecionar o nível de permissão e informar o código do cartão para um novo cadastro, após esse processo, poderá clicar em “Gerar token”. Esta ação somente o usuário com nível de administrador do sistema terá acesso.

Figura 37. Tela mostra token.



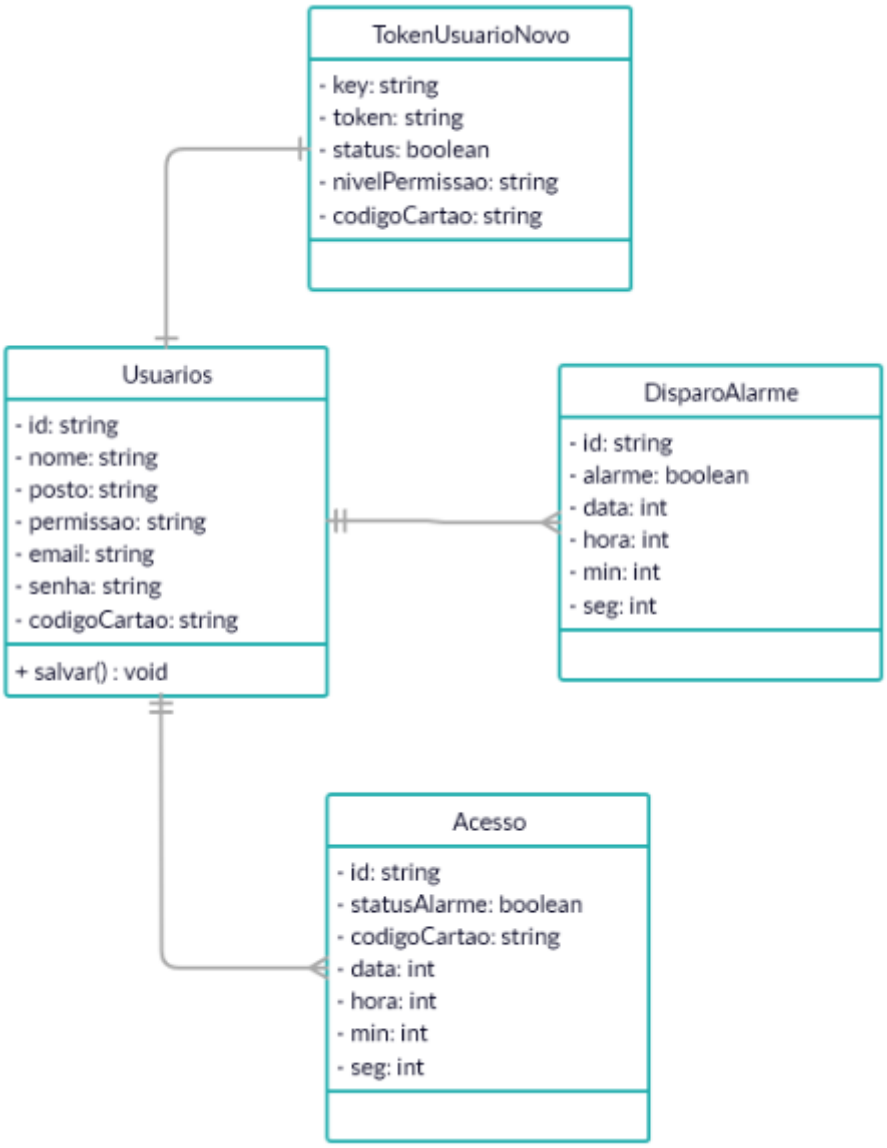
Fonte: Desenvolvido pelo autor.

O usuário só poderá gerar novo token depois que o último token gerado for utilizado, por isso logo após ocorrer a geração do token o botão “Gerar token” é desabilitado. Nesta tela são informados todos os dados necessários para a gestão do token, conforme Figura 37.

Apesar de ser um sistema complexo envolvendo o desenvolvimento de um aplicativo mobile que se comunica com um dispositivo IoT, as classes modelo

que precisaram persistir no banco de dados foram apenas 4, apresentadas no diagrama de classes da Figura 38.

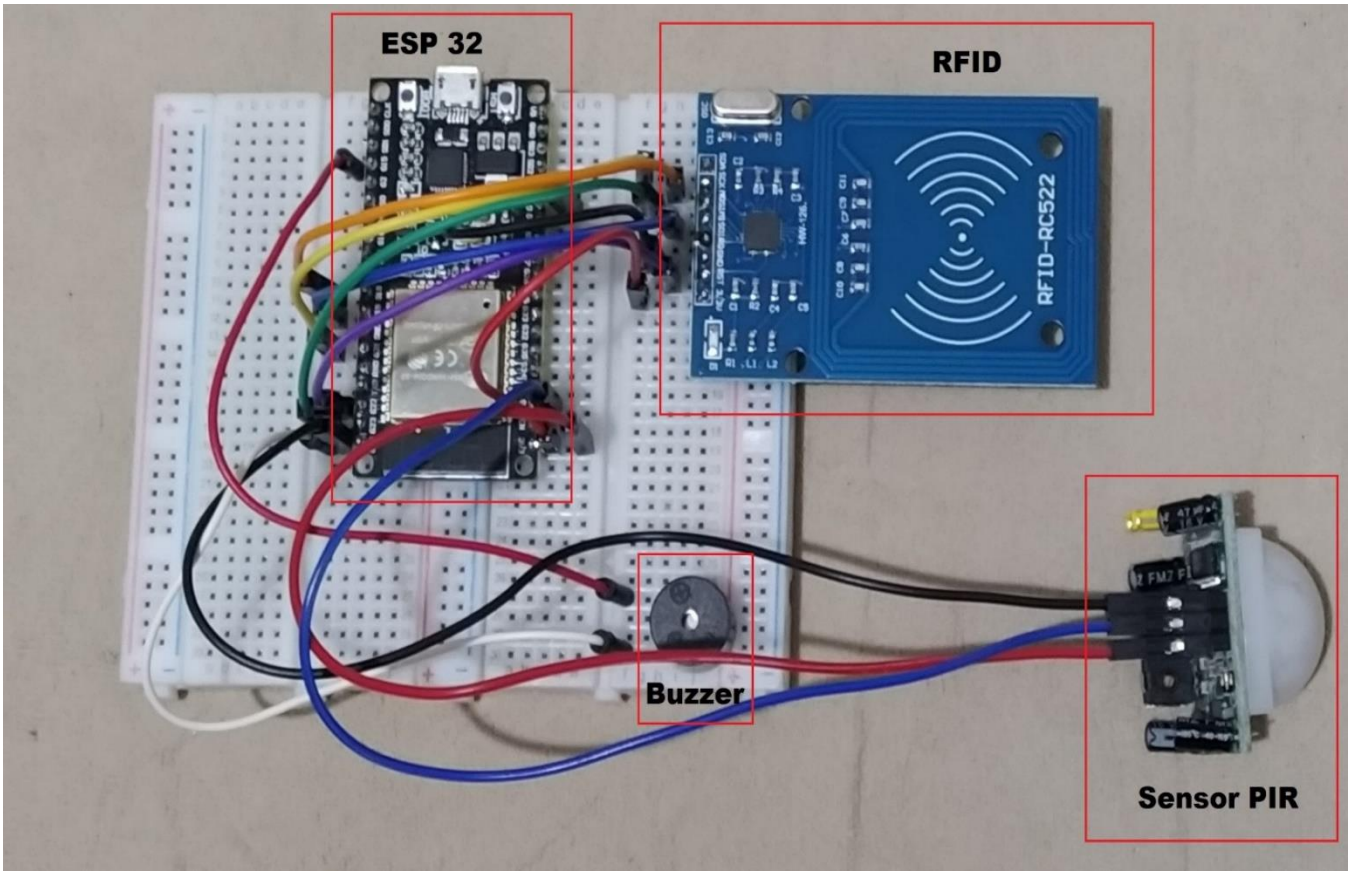
Figura 38. Diagrama de classes.



Fonte: Desenvolvido pelo autor.

No dispositivo IoT a comunicação dos sensores com o microcontrolador é feita a partir das portas GPIO, portanto sua configuração física ficou da seguinte forma: As portas 21 e 22 fazem a comunicação do RFID, o sensor PIR a 36, pôr fim a porta 15 para o Buzzer, conforme Figura 39.

Figura 39. Dispositivo IoT.



Fonte: Desenvolvido pelo autor.

O objetivo do componente Buzzer no projeto é apenas a sinalização da mudança do status do alarme toda vez que uma TAG é aplicada no sensor RFID. Foi configurado para emitir 1 bip quando o alarme muda seu status para ativado, 2 bips para o desativado e 3 bips quando uma TAG não cadastrada é aplicada.

4.5 Validação do Projeto

Foi realizado um teste de funcionalidade do sistema com os possíveis usuários, os mesmos anteriormente entrevistados, na fase de coleta dos requisitos da seção 4.1. As avaliações são apresentadas nas tabelas 4 e 5 a seguir.

Tabela 4. Teste e avaliação de usabilidade - Superiores

Perguntas Superior	1°CRPM	COE	CHOQUE
	Respostas		
O aplicativo é claro e intuitivo?	Sim	Sim	Sim
Observações e sugestões de melhoria	Alarme sonoro	Câmera	Biometria
Pontue a sua satisfação quanto à usabilidade do projeto - 0 a 5. 0 – Totalmente insatisfeito, 5 – Totalmente satisfeito.	5	5	5

Fonte: Desenvolvido pelo Autor

A princípio quatro departamentos participaram da coleta de requisitos através da aplicação dos questionários da seção 4.1. Neste segundo momento, o BOPE não foi incluído na validação do trabalho, pois o superior direto havia relatado que o fluxo na área deste depósito era reduzido, portanto definiu como não necessária a participação nesse desenvolvimento e validação.

A tabela 4 corresponde as respostas dos superiores quanto a funcionalidade do sistema. Primeiramente foi apresentado o projeto completo, onde foi possível utilizar o aplicativo realizando cadastros, geração de token, exclusão de usuários, geração de notificação de disparo e visualização de relatórios; foi demonstrado também o sensor de movimento e utilização da TAG. O objetivo foi proporcionar uma experiência sobre a abrangência do projeto, perante as necessidades dos usuários, para então posteriormente colher a satisfação e sugestões.

Os superiores relataram que o projeto soluciona as principais dificuldades da função, promove um melhor gerenciamento das informações, facilita identificação de soldados, propicia de fato maior segurança tanto aos materiais quanto às pessoas envolvidas no processo. Além desses gerenciamentos foi destacado que será possível otimizar a hora de trabalho, pois os furriéis poderão utilizar melhor o tempo, um exemplo é nas reservas com monitoramento 24 horas, as jornadas de trabalho poderão ser reduzidas, deixando parte desse serviço a cargo do sistema.

As sugestões para futuros trabalhos foram incluir mais dispositivos, como alarme sonoro, câmeras e acesso as portas por biometria.

Tabela 5. Teste e avaliação de usabilidade - Furriéis

Perguntas Furriel	**1º CRPM**	**COE**	**CHOQUE**
	Respostas		
O aplicativo é claro e intuitivo?	Sim	Sim	Sim
Observações e sugestões de melhoria	Alarme sonoro	Trava física	Ímã na porta
Pontue a sua satisfação quanto à usabilidade do projeto - 0 a 5. 0 – Totalmente insatisfeito, 5 – Totalmente satisfeito.	5	5	5

Fonte: Desenvolvido pelo Autor

A apresentação do projeto completo ocorreu da mesma forma a todos os envolvidos, possibilitando a mesma oportunidade de experiência com o sistema. Os furriéis, conforme a tabela 5, também validaram a funcionalidade do trabalho.

De forma geral relataram que este projeto deve ser apresentado a todo o comando da PMPR, para que seja implementado de fato em todas as áreas que possuem materiais bélicos, pois visualizam a solução como efetiva no aumento da segurança. Além de tudo foi citado que o aplicativo tem um design intuitivo e bom desempenho.

As sugestões para trabalhos futuros foram a implementação de alarme sonoro, trava física nas portas com, por exemplo, tranca de aço e ímãs. Na primeira entrevista foram sugeridos os dispositivos de biometria, sensor de movimento e controle por smartphone do sistema. Foi visto que nessa segunda pesquisa, as sugestões tiveram maior variedade, pois os usuários puderam compreender melhor as possibilidades geradas pelo projeto, através da experiência de utilização.

5. CONCLUSÃO E TRABALHOS FUTUROS

Este projeto foi desenvolvido em sua totalidade conforme o que foi proposto, entretanto, cada reserva de armamento possui uma estrutura física diferenciada das demais, com isso, esse projeto foi desenvolvido de forma física genérica e testado nos ambientes interessados. Através do levantamento de casos de extravio de armamento, estudo dos processos de segurança e a realização de entrevistas com os responsáveis dos setores, foi possível estabelecer os requisitos e recursos necessários ao projeto, visando o desenvolvimento mais adequado para satisfazer as necessidades destas reservas de material bélico.

Por fim, gerou-se um aplicativo móvel, um dispositivo IoT e um banco de dados que trabalham com eficiência e confiabilidade, entregando maior segurança e monitoramento no interior das reservas de armamento, gerando notificações no aplicativo móvel a respeito de possíveis invasões e gerando relatórios de acesso e disparos do alarme. Essa base de dados poderá futuramente ser populada com dados reais. Além dos resultados dos objetivos previamente estabelecidos, pode-se desenvolver também o gerenciamento de usuários, onde é possível realizar o cadastramento, divisão de níveis de permissão e exclusão.

O projeto fornece segurança e monitoramento, comprovadamente eficiente segundo o teste e avaliação de usabilidade, realizado com os furriéis e superiores. Os usuários puderam utilizar o aplicativo com totalidade das funcionalidades, afirmaram de modo geral que o aplicativo é intuitivo, com design e layout limpo, fornece todas as informações necessárias para o gerenciamento e que entendem a importância de futuras aplicações reais na PMPR. As sugestões citadas foram para a introdução de câmeras, identificação biométrica, alarme sonoro e trava física. Na análise de satisfação quantitativa, a nota máxima foi obtida unanimemente.

O projeto focou em atender as necessidades prioritárias dos policiais que realizam a guarda das áreas de materiais bélicos. Essa solução viabiliza uma maior segurança e gestão, com custo reduzido, pois contempla dispositivos de baixo custo e alta eficácia. O custo desses equipamentos é de aproximadamente 100 reais, esse valor não inclui o tempo de desenvolvimento

do aplicativo e a estrutura do projeto. Conforme a apresentação para comandantes e possível implementação real deste sistema, as sugestões e as necessidades de cada local serão avaliadas para determinar uma construção coerente e eficaz.

5.1 TRABALHOS FUTUROS

De acordo com as entrevistas de coleta de requisitos e de validação do projeto, foram extraídas algumas ideias para trabalhos futuros, visando a continuidade e implementação. As sugestões são: uma câmera no dispositivo IoT que seja acessível pelo aplicativo móvel, para que possa visualizar em tempo real o interior da reserva de material; a substituição do sensor RFID por um leitor de impressão digital, em que o cadastro da biometria seja feita tanto pelos smartphones que possuem esse dispositivo, como também diretamente no leitor biométrico da reserva; inclusão da possibilidade de interface do sistema com travas físicas, tais como travas magnéticas de portas; inclusão da possibilidade do dispositivo IoT disparar ou emitir alarmes sonoros no momento de um acesso não autorizado. Também foi observada a necessidade da implementação de uma opção para envio do relatório para o e-mail. Na parte do cadastro do usuário, foi constatada a importância de uma confirmação da senha e sua recuperação, no caso de esquecimento. No dispositivo IoT existe a necessidade da configuração de sua rede Wi-Fi a partir do aplicativo móvel, para que o dispositivo possa acessar a rede específica pertencente a reserva onde será implementado.

6. REFERÊNCIAS

BRASIL. Decreto n. 7339, de 8 de jun. 2010. **Aprova o Regulamento Interno e dos Serviços Gerais da PMPR. Lex**: Diário Oficial: Secretaria de Estado da Segurança Pública - SESP, Estado do Paraná, p. 160-170, jun. 2010. Legislação Estadual.

SANTOS, Tiago. **Tendências e inovação com computação em nuvem**. 1. Ed. São Paulo: Senac São Paulo, 2019. 152 p.

MOREIRA, Matheus. **Em 8 anos, 600 armas da marca Taurus foram roubadas ou extraviadas da PM de SP**. 2018. Disponível em: <https://ponte.org/em-8-anos-600-armas-da-marca-taurus-foram-roubadas-ou-extraviadas-da-pm-de-sp/>. Acesso em: 13 dez. 2019.

RANGEL BANDEIRA, Antônio. **Ranking dos Estados no Controle de Armas: Análise Preliminar Quantitativa e Qualitativa dos Dados sobre Armas de Fogo Apreendidas no Brasil.** 2008. Disponível em:<https://congressoemfoco.uol.com.br/upload/congresso/arquivo/mapa_das_armas_brasil.pdf>. Acesso em 12 dez. 2019.

NETO, Kfouri Miguel. **TJ-PR, Tribunal de Justiça do Paraná - Apelação: APL 13576548 PR 1357654-8.** 2015. Disponível em:<https://tj-pr.jusbrasil.com.br/jurisprudencia/204182092/apelacao-apl-13576548-pr-1357654-8-acordao?ref=juris-tabs>. Acesso em 14 dez. 2019.

VIANA, Daniel. **Firebase: descubra no que esta plataforma pode te ajudar.** Treinaweb Blog, janeiro de 2017. Disponível em: <https://www.treinaweb.com.br/blog/firebase-descubra-no-que-esta-plataforma-pode-te-ajudar/>. Acesso em: 13 jun. 2020.

HARADA, Eduardo. **O que é o Android Studio, ferramenta criada para desenvolver apps mobile.** Tecmundo Udemy, setembro de 2019. Disponível

em: <https://www.tecmundo.com.br/software/146361-o-android-studio-ferramenta-criada-desenvolver-apps-mobile.htm>. Acesso em: 13 jun. 2020.

MOTA, Allan. **O que é Arduino e como funciona.** Portal vida de Silício, maio de 2017. Disponível em: <https://portal.vidadesilicio.com.br/o-que-e-arduino-e-como-funciona/>. Acesso em: 13 jun. 2020.

STRAUB, Matheus Gebert. **Arduino IDE – O software para gravação de códigos no Arduino.** USINAINFO Blog, outubro de 2019. Disponível em: <https://www.usinainfo.com.br/blog/arduino-ide-o-software-para-gravacao-de-codigos-no-arduino/>. Acesso em: 13 jun. 2020.

LOCATELLI, Caroline. **Conhecendo o Esp32.** Blog curto circuito, 2020. Disponível em: <https://www.curtocircuito.com.br/blog/conhecendo-esp32 >. Acesso em: 13 jun. 2020.

REIS, Fábio dos. **Como funciona um Sensor de Movimento PIR – Passive Infrared**. Boson treinamentos, dezembro de 2018. Disponível em: <http://www.bosontreinamentos.com.br/eletronica/como-funciona-um-sensor-de-movimento-pir-passive-infrared/>. Acesso em: 13 jun. 2020.

CIRIACO, Douglas. **Como funciona a RFID.** Tecmundo, agosto de 2009. Disponível em: <https://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm>. Acesso em: 13 jun. 2020.

CORREA, Gunnar. **Beep usando Buzzer com Arduino**. SatellaSoft, março de 2015. Disponível em: <https://www.satellasoft.com/?materia=beep-usando-buzzer-com-arduino>. Acesso em: 23 jun. 2020.

KOYANAGI, Fernando. **Sensor de presença com NodeMCU ESP8266**. Fernando K Tutoriais, Tecnologia, Tendências, novembro de 2017. Disponível em: <https://www.fernandok.com/2017/11/sensor-de-presenca-com-nodemcu-esp8266.html >. Acesso em: 25 jun. 2020.

Sensor de presença PIR - HC-SR501. ROBOCORE, OnlineStore. Disponível em: <https://www.robocore.net/loja/sensores/sensor-de-presenca-pir-hc-sr501?gclid=EAIaIQobChMIvC_ouaW6gIVlYWRCh38PwBNEAQYASABEgLUXfD_BwE >. Acesso em: 25 jun. 2020.

7. APÊNDICES

7.1 APÊNDICE A – GRÁFICO DE GANTT PARTE 1

Mês	novembro		Dezembro		Janeiro				Fevereiro			
Dias	18 a25	25 a 2	9 a 16	16 a 23	2 a 9	9 a 16	16 a 23	23 a 30	30 a 6	6 a 13	13 a 20	20 a 27
Semanas	1	2	3	4	5	6	7	8	9	10	11	12
Definição do tema												
Entrega do tema												
Pesquisa Documentação/Coleta de dados												
Formulação de Questionário para Entrevista												
Coleta de Requisitos: Entrevistas												
Pesquisa dados Vajme/Coger												
Desenvolvimento Documentação - Corpo do trabalho TCC												
Marco 1: 1º Entrega Documentação 18/12/2019												
Definir funcionalidade do App												
Interface gráfica básica - Android												
Login com Firebase - Android												
Autenticação Firebase - Android												
Interface do Menu - Android												
Lógica de programação básica - Android												
Teste e validação 1º Fase												
Marco 2: 1º Fase Desenvolvimento Android												
Programação leitor RFID												
Programação Sensor de movimento												
Lógica de programação - Integração sensores												
Configuração rede Wifi												
Envio dos dados para Firebase												
Teste e Validação IoT												
Marco 3: Desenvolvimento IoT ESP32												
Interface gráfica avançada do menu												
Desenvolvimento Menu												
Desenvolvimento "Relatórios de acessos e disparos"												
Status do alarme												
Tags cadastradas												
Envio e leitura de dados via Firebase												
Teste e Validação Desenvolvimento Android												
Marco 4: 2º Fase Desenvolvimento Android												
Validação do projeto												
Ajustes finais												
Entrega Final												

Fonte: Desenvolvido pelo autor.

7.2 APÊNDICE B – GRÁFICO DE GANTT PARTE 2

Mês	Março				Abril					Maio				Junho				
Dias	27 a 5	5 a 12	12 a 19	19 a 26	26 a 2	2 a 9	9 a 16	16 a 23	23 a 30	30 a 7	7 a 14	14 a 21	21 a 28	28 a 4	4 a 11	11 a 18	18 a 25	25 a 30
Semanas	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Definição do tema																		
Entrega do tema																		
Pesquisa Documentação/Coleta de dados																		
Formulação de Questionário para Entrevista																		
Coleta de Requisitos: Entrevistas																		
Pesquisa dados Vajme/Coger																		
Desenvolvimento Documentação - Corpo do trabalho TCC																		
Marco 1: 1º Entrega Documentação 18/12/2019																		
Definir funcionalidade do App																		
Interface gráfica básica - Android																		
Login com Firebase - Android																		
Autenticação Firebase - Android																		
Interface do Menu - Android																		
Lógica de programação básica - Android																		
Teste e validação 1º Fase																		
Marco 2: 1º Fase Desenvolvimento Android																		
Programação leitor RFID																		
Programação Sensor de movimento																		
Lógica de programação - Integração sensores																		
Configuração rede Wifi																		
Envio dos dados para Firebase																		
Teste e Validação IoT																		
Marco 3: Desenvolvimento IoT ESP32																		
Interface gráfica avançada do menu																		
Desenvolvimento Menu																		
Desenvolvimento "Relatórios de acessos e disparos"																		
Status do alarme																		
Tags cadastradas																		
Envio e leitura de dados via Firebase																		
Teste e Validação Desenvolvimento Android																		
Marco 4: 2º Fase Desenvolvimento Android																		
Validação do projeto																		
Ajustes finais																		
Entrega Final																		

Fonte: Desenvolvido pelo autor.